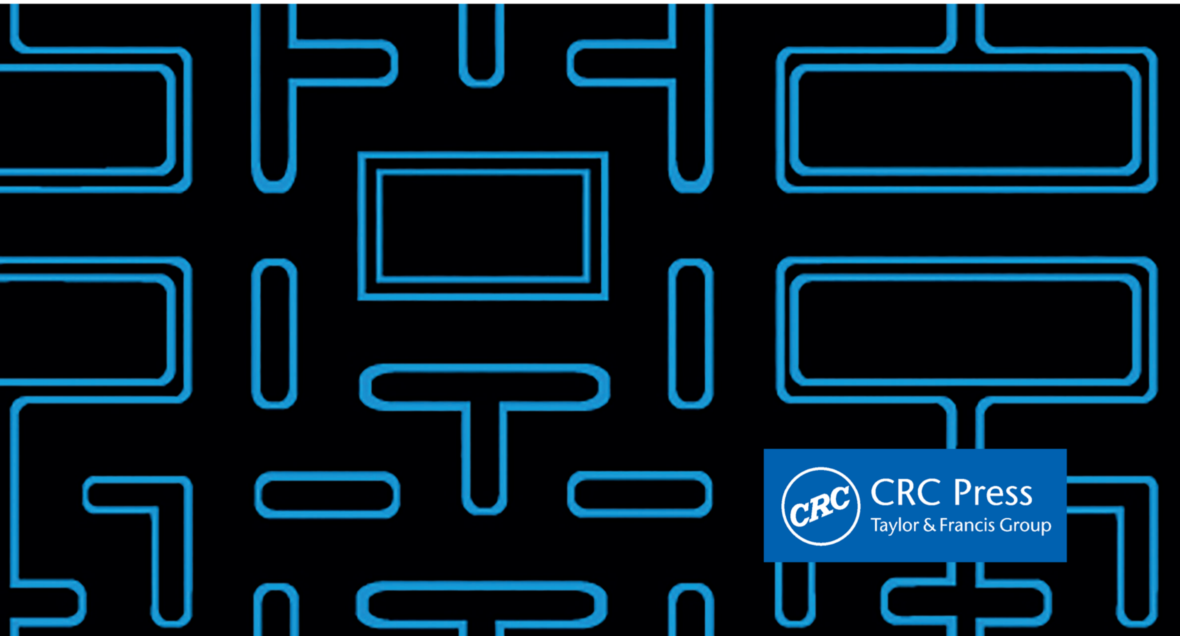
NUMBER THEORY AND ITS APPLICATIONS

Satyabrota Kundu and Supriyo Mazumder



CRC Press
Taylor & Francis Group

Number Theory and its Applications

Satyabrota Kundu
Supriyo Mazumder

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

LEVANT

Levant Books
India

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Dedicated to our Family Members.

First published 2022
by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

© 2022 Satyabrota Kundu and Supriyo Mazumder

CRC Press is an imprint of Informa UK Limited

The right of Satyabrota Kundu and Supriyo Mazumder to be identified as authors of this work has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Print edition not for sale in South Asia (India, Sri Lanka, Nepal, Bangladesh, Pakistan or Bhutan).

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested

ISBN: 9781032231433 (hbk)
ISBN: 9781003275947 (ebk)

DOI: 10.1201/9781003275947

Typeset in Knuth Computer Modern 10.5 pt
by Levant Books

LEVANT

Preface

From ancient times, number theory has always occupied the unquestioned historical importance of the subject. Number Theory is both pure and applied and at the same time both classical and modern. It has been the objective of the authors for quite some time to write an accessible and inviting textbook to number theory. Foremost, the present textbook will create an effective instrument for both teaching and learning. The authors aim to integrate the richness and beauty of the subject and at the same time the book is full of unexpected usefulness. In the present text, the authors have worked hard to assemble many contrasting aspects of number theory into one standard textbook.

This book is ideal for undergraduate and postgraduate level students. Certain levels of mathematical reasoning, basic algebra and real analysis are required as prerequisites to study the materials of our textbook. This textbook is designed in such a manner that it will serve the purpose for a wide range of readers.

Some effort has been devoted to make the first few chapters less challenging, but gradually the chapters become more challenging. At each juncture, the instructor has to decide how deeply to pursue a particular topic before moving ahead to a new one.

Chapter I introduces important topics like well-ordering property, principle of mathematical induction, Binomial theorem and many more in establishing results to study the materials of the textbook.

Chapter II introduces the notion of divisibility, where with the help of the Euclidean algorithm, the greatest common divisors of a set of integers are introduced. Also the least common multiple and linear Diophantine equations are discussed.

Chapter III deals with prime factorization, the fundamental theorem of arithmetic and factorization techniques are covered.

Chapter IV introduces congruences and develops their fundamental properties. systems of linear congruences in one or more unknowns are discussed. The Chinese remainder theorem is also developed.

Chapter V is concerned with Fermat's Little theorem and Wilson's theorem. Wilson's theorem gives a congruence for factorials. Pseudo primes, strong pseudoprimes and absolute pseudoprimes(Carmichael numbers) are also introduced.

Chapter VI gives a thorough discussion of the sum and number of divisors, M$\ddot{o}$bius function and greatest integer function.

Chapter VII develops Euler's ϕ-function, Euler's theorem and properties of Euler's ϕ-function. Explicit formulae are developed for these functions.

Chapter VIII is devoted to the discussion of the order of an integer and of the primitive roots. Indices, which are similar to logarithms, are introduced. Primality testing based on primitive roots are described.

Chapter IX includes discussions on quadratic residues and the famous law of quadratic reciprocity. The Legendre and Jacobi symbols are introduced and algorithms for evaluating them are described.

Chapter X deals with Integers of Special forms where the special emphasis is given on Perfect numbers, Mersenne primes and Fermat's numbers.

Chapter XI treats simple finite and infinite continued fractions. Special attention is paid to the Periodic fractions.

Chapter XII covers the study on few non-linear Diophantine equations, where the various results on Pythagorean triples and Fermat's Last theorem are done.

Chapter XIII deals with the study of Integers as sum of squares, which includes sum of two squares and sum of more than two squares.

Concluding chapter introduces the application part of number theory, where the Fibonacci numbers, Pseudo-random numbers and basic cryptology have been discussed. Here the Pseudo-random numbers and the techniques for generating them are discussed. In cryptology, Caeser cipher, Block cipher, Exponentiation cipher and RSA are based on modular arithmetic.

After each section of the text there are worked-out exercises set containing problems of various levels of difficulty. Each set contains problems of a numerical nature, which should be done to develop computational skills. At the end of every chapter there is an exercise set to fine-tune the practice for the students. Throughout the textbook, the readers will face some simple questions like Why! and Verify! to make the topics interesting for them to study. At the end of the textbook there is an extensive bibliography, where the lists of number theory texts and references are included for interested readers who would like to go for more details about some of the topics covered in the book.

Finally, the authors would like to express their heartfelt gratitude to their respected teachers, friends and relatives, who provide constant support and inspiration in framing the book.

Contents

1 Prerequisites **1**

2 Theory of Divisibility **15**

2.1 Introduction 15
2.2 Divisibility 16
2.3 Worked out Exercises 20
2.4 Greatest Common Divisor 23
2.5 Least Common Multiple 31
2.6 Worked out Exercises 33
2.7 Linear Diophantine Equations 37
2.8 Worked out Exercises 39
2.9 Exercises: 42

3 Prime Numbers **45**

3.1 Introduction 45
3.2 Primes & Fundamental Theorem of Arithmetic 46
3.3 Worked out Exercises 56
3.4 Exercises: 65

4 Theory of Congruences **67**

4.1 Introduction 67
4.2 Congruences 68
4.3 Worked out Exercises 73
4.4 Linear Congruences 77
4.5 Worked out Exercises 81
4.6 System of Linear Congruences 87
4.7 Worked out Exercises 91
4.8 Exercises: 92

5 Fermat's Little Theorem 95

5.1 Introduction 95
5.2 Fermat's Little Theorem 96
5.3 Worked out Exercises 101
5.4 Wilson's Theorem 106
5.5 Worked out Exercises 108
5.6 Exercises: 110

6 Arithmetic Functions 113

6.1 Introduction 113
6.2 The Sum and Number of Divisors 114
6.3 Worked out Exercises 118
6.4 Mobi$\ddot{u}$s μ-function 126
6.5 Worked out Exercises 129
6.6 Greatest Integer Function 132
6.7 Worked out Exercises 137
6.8 Exercises: 143

7 Euler's Generalization and ϕ–function 145

7.1 Introduction 145
7.2 Euler's ϕ–function 146
7.3 Worked out Exercises 149
7.4 Euler's Theorem 153
7.5 Worked out Exercises 155
7.6 Properties of ϕ–function 158
7.7 Worked out Exercises 161
7.8 Exercises: 165

8 Primitive Roots 167

8.1 Introduction 167
8.2 Multiplicative Order 168
8.3 Worked out Exercises 171
8.4 Primitive Roots for Primes 175
8.5 Worked out Exercises 179
8.6 Existence of Primitive Roots 183
8.7 Worked out Exercises 188
8.8 Index Arithmetic 192
8.9 Worked out Exercises 197
8.10 Exercises: 200

9 Theory of Quadratic Residues **203**
9.1 Introduction . . . 203
9.2 Quadratic Residues and Nonresidues . . . 203
9.3 Worked out Exercises . . . 212
9.4 Quadratic Reciprocity Law . . . 217
9.5 Worked out Exercises . . . 221
9.6 The Jacobi Symbol . . . 225
9.7 Worked out Exercises . . . 232
9.8 Exercises: . . . 235

10 Integers of Special Forms **239**
10.1 Introduction . . . 239
10.2 Perfect Numbers . . . 239
10.3 Worked out Exercises . . . 244
10.4 Mersenne Primes . . . 247
10.5 Worked out Exercises . . . 254
10.6 Fermat Numbers . . . 257
10.7 Worked out Exercises . . . 261
10.8 Exercises: . . . 263

11 Continued Fractions **265**
11.1 Introduction . . . 265
11.2 Finite Continued Fractions . . . 266
11.3 Worked out Exercises . . . 273
11.4 Infinite Continued Fractions . . . 276
11.5 Worked out Exercises . . . 284
11.6 Periodic Fractions . . . 286
11.7 Worked out Exercises . . . 292
11.8 Exercises: . . . 293

12 Few Non-Linear Diophantine Equations **295**
12.1 Introduction . . . 295
12.2 Pythagorean Triples . . . 296
12.3 Worked out Exercises . . . 299
12.4 Fermat's Last Theorem . . . 302
12.5 Worked out Exercises . . . 303
12.6 Exercises: . . . 306

13 Integers as Sums of Squares **307**
13.1 Introduction 307
13.2 Sum of Two Squares 307
13.3 Worked out Exercises 312
13.4 Sum of More than Two Squares 315
13.5 Worked out Exercises 319
13.6 Exercises: 321

14 Certain Applications on Number Theory **323**
14.1 Fibonacci Numbers 323
14.2 Worked out Exercises 331
14.3 Pseudo-random Numbers 334
14.4 Worked out Exercises 338
14.5 Cryptology 339
14.6 Worked out Exercises 346
14.7 Exercises: 348

Bibliography **351**

Index **353**

1

Prerequisites

Number theory is an important and significant area of Mathematics. From ancient times, it has had a substantial impact on human civilization. For further development many great philosophers had contributed various aspects of number theory. Among those was Pythagoras ($569 - 500$ B.C). His famous Pythagorean theorem led many mathematicians to study squares and sum of squares. He has given us notable Pythagorean triplets. After 200 years, another Greek mathematician Euclid (350 B.C.) drew attention to the prime numbers. His investigations were based on the renowned Euclidean algorithm for finding greatest common divisors of two natural numbers. It plays a key role for evaluating prime factorisation of natural numbers. Few more studies on natural numbers had been done by Eratosthenes(276B.C.-196B.C.), Nicomachus(C.100) and Diophantus(C.250). The study of number theory started with the set of natural numbers, denoted by $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$. Two basic operations addition and multiplication are defined on $\mathbb{N}$. But in general, the subtraction is not defined. The reason behind this is that the people will not be able to take Rs 5 from a person with Rs 4. Thus for $u, v \in \mathbb{N}$, $u - v$ is not always defined. Here comes the notion of negative natural numbers that is $-1, -2, -3, \ldots$ so on. Therefore the set $\{1, 2, 3, 4, \ldots, -1, -2, -3, -4, \ldots\}$ is an enlargement of $\mathbb{N}$. But here 0 is missing. The concept of zero originated in ancient India, ancient Babylon and the Mayan civilisation. It is believed that it came into existence from 458 A.D. Actually the concept of zero was developed at different times in each of these civilisations. But it was first used in ancient India by Hindus and thereby Arabics use it as a number. Thus by inclusion of zero and the negative natural numbers create a new set known as set of integers, denoted by $\mathbb{Z} = \{-1, -2, -3, -4, \ldots, 0, 1, 2, 3, 4, \ldots\}$. Here the basic operations addition, subtraction and multiplication is possible. But division, the inverse operation of multiplication is not defined on $\mathbb{Z}$. In other words, if u, v are elements of $\mathbb{Z}$ then $\frac{u}{v}$ is not always an element of $\mathbb{Z}$. The set of integers plays an important role in the study of number theory. Next we proceed with our discussion by two important properties of natural numbers or sets of positive integers. The first begins with a well ordering principle.

The Well-Ordering Property: Every nonempty subset A of natural numbers has a least element. In other words, if A is a non-empty subset of $\mathbb{N}$ then $\exists\ m \in A$ such that $m \leq a$, $\forall a \in A$. In particular, $\mathbb{N}$ itself has the least element 1.

We now prove these two principles by taking help of each other. First we will prove the well-ordering principle using the principle of mathematical induction.

(I)Deduction of mathematical induction by well ordering principle.

Proof. Let A be the subset of natural numbers where $1 \in A$ and if $k \in A$ then $k + 1 \in A$. Its suffices to show that $A = \mathbb{N}$. To fulfill this, let B be the set of those natural numbers which does not belong to A. Then $A \cup B = \mathbb{N}$ and $A \cap B = \phi$. To get the desired result we need to show that $B = \phi$. If possible, let $B \neq \phi$. Then by well ordering principle there exists a least element m of B such that $m \leq n$, $\forall\ n \in B$. Note that $1 \neq m$ as $1 \in A$ and hence $1 \notin B$. Since m is the least element of B, therefore $m - 1 \notin B$ and this gives $m - 1 \in A$. By hypothesis, we have $(m - 1) + 1 \in A$ *i.e.* $m \in A$. This contradicts the fact that $A \cap B = \phi$. So our assumption that $B \neq \phi$ is wrong. This proves that $A = \mathbb{N}$. ☐

(II) Deduction of well-ordering principle by mathematical induction.

Proof. To the contrary, let A be the non empty subset of $\mathbb{N}$ having no least element. Let us construct a set B of natural numbers in such a way that any number $x \in B$ is less than every member of A. Thus $B = \{x | x \in \mathbb{N}\ \&\ x < a\}$ for every $a \in A$. Then every member of A is either greater than or equal to each member of B. Therefore $A \cap B = \phi$. Note that $1 \notin A$, otherwise 1 will become the least element of A. But by hypothesis A has no least element. Therefore $1 \in B$ and $1 < a$ for every $a \in A$.

Assume that $t \in B$. Then $t < a$ for every $a \in A$. We assert $t + 1 \notin B$. If so, then $t + 1$ be the next natural number larger than t. Then $t + 1$ will be the least element of A but A does not have any least element. Hence $t + 1 \in B$. Hence by principle of mathematical induction $B \subseteq \mathbb{N}$. But $A \cap B = \phi$. Then $\mathbb{N} \cap A = \phi$ yields $A = \phi$, a contradiction. Therefore A must have a least element. This completes the proof. ☐

The above discussion leads to the following theorems related to mathematical induction.

Theorem 1.0.1. *Principle of induction: Let S be a subset of $\mathbb{N}$ such that*

(i) $1 \in S$,

(ii) *if $k \in S$, then $k+1 \in S$. Then $S = \mathbb{N}$.*

Theorem 1.0.2. *Let $P(n)$ be u statement with $n \in \mathbb{N}$ satisfying*

(i) $P(1)$ *is true,*

(ii) $P(k+1)$ *is true, whenever $P(k)$ is true; then $P(n)$ holds for all n.*

Example 1.0.1. *Prove that for each $n \geq 2$, $(n+1)! > 2^n$. The inequality holds for $n = 2$ since $(2+1)! > 2^2$.*

Solution 1.0.1. *Let the inequality hold for some natural number $k \geq 2$. Then $(k+1)! > 2^k$. We are to prove that the inequality prevails for $k+1$ ı.e. $\{(k+1)+1\}! > 2^{k+1}$. Now*

$$\begin{aligned} \{(k+1)+1\}! = (k+2)! &= (k+2)(k+1)! \\ &> 2 \cdot 2^k [\because\ k+2 > 2] \\ &= 2^{k+1}. \end{aligned}$$

Hence the inequality prevails for $k+1$. Therefore by principle of induction, the inequality holds for all natural numbers ≥ 2.

Remark 1.0.1. *It is to be noted that the inequality fails to hold for $n = 1$.*

Example 1.0.2. *Prove that for every $n \geq 1$,*

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Solution 1.0.2. *Let $P(n) : \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ be the statement for $n \geq 1$. Note that $P(1)$ is true(Verify!). Let k be the positive integer such that $P(k)$ holds. We are to show $P(k+1)$ holds. Now*

$$\begin{aligned} &\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}, \because\ P(k) \textit{ holds} \\ &= \frac{1}{k+1} \cdot \frac{(k+1)^2}{k+2} \\ &= \frac{k+1}{(k+1)+1}. \end{aligned}$$

Hence $P(k+1)$ holds. Hence the result follows.

Example 1.0.3. *Prove that* $2m+1<2^m$ *for all integers* $m\geq 3$.

Solution 1.0.3. *Let* $P(m): 2m+1<2^m$ *be the statement, for all integers* $m\geq 3$. *Here for* $m=3$, *we have* $2\cdot 3+1=7<8=2^3$. *Thus the statement is true for* $m=3$. *Hence* $P(3)$ *holds. Suppose* $k(\geq 3)$ *is an integer for which the statement* $P(k)$ *is true. To prove the validity of the argument of this statement we need to show* $P(m)$ *is true for* $m=k+1$. *Now*

$$\begin{aligned}2(k+1)+1 &= 2k+1+2\\ &< 2^k+2[\textit{Since } P(m) \textit{ is true for } m=k]\\ &< 2^k+2^k[\textit{since } k\geq 3]\\ &< 2^{k+1}.\end{aligned}$$

Thus the statement $P(m)$ *is true for* $m=k+1$. *So by applying the principle of mathematical induction, we can say that* $P(m)$ *is true for all* $m\geq 3$.

Example 1.0.4. *Prove that* $n^2<2^n$ *for every integers* $n\geq 5$.

Solution 1.0.4. *Let* $P(n): n^2<2^n$ *be the given statement for all integers* $n\geq 5$. *Here* $P(5)$ *is true(verify!). Suppose* k *is a positive integer such that* $k\leq 5$ *and* $P(k)$ *is true. We are to show* $P(k+1)$ *is true. Now*

$$\begin{aligned}(k+1)^2=k^2+2k+1 &< 2^k+2k+1(\textit{by induction hypothesis})\\ &< 2^k+2^k(\textit{see Example 1.0.3})\\ &< 2\cdot 2^k=2^{k+1}.\end{aligned}$$

So $P(k+1)$ *holds. Hence this finishes the result.*

As we know counting is an important aspects of number system. There is a deep and significant relation between counting techniques and number theory. We now continue our discussion with a significant property of counting techniques, Pigeonhole principle, of the set of integers $\mathbb{Z}$. It plays a key role in the study of numbers. The statement of this principle as follows.

Theorem 1.0.3. *Pigeonhole principle: The simplest form of the principle is that, if* $k+1$ *or more objects are to be placed in* k *boxes then there is at least one box containing two or more of the objects.*

Proof. In anticipation of a contradiction, suppose that none of the k boxes has more than one object. Then the total number of objects will be k. This would lead to the contradiction as there are $k+1$ or more objects. □

In fact the first formalisation of the notion of Pigeonhole principle is believed to be given by Dirichlet$(1805-1859)$. He called it as drawer principle. But the term "Pigeonhole principle "was first coined by the mathematician Raphael M. Robinson in 1940. The next example illustrates this concept lucidly.

Example 1.0.5. *If there is a group of* 368 *people in a club, then there must be at least three people with the same birthday. The reason behind this is that the number of possibilities of birthdays in a year is* 366*.*

One can think that this principle is very much obvious. But this in fact would become an useful tool once we generalize it. The statement of this generalization is as follows:

If n objects are placed in k boxes, then there is at least one box containing at least $\left[\frac{n}{k}\right]$ number of objects, where $\left[\frac{n}{k}\right]$ is the greatest integer not exceeding $\frac{n}{k}$.

Another important aspect of counting techniques which can be used frequently in the study of number theory is binomial theorem and it can be stated as follows.

Theorem 1.0.4. *For any two real numbers a, b and any positive integer n,*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^n b^{n-r}.$$

One of the nice diagrammatic representation of binomial coefficients is Pascal's triangle, named after French mathematician Blaise Pascal. This looks like

$$\begin{array}{lccccccccccccc}
n=0 & & & & & & & 1 & & & & & & \\
n=1 & & & & & & 1 & & 1 & & & & & \\
n=2 & & & & & 1 & & 2 & & 1 & & & & \\
n=3 & & & & 1 & & 3 & & 3 & & 1 & & & \\
n=4 & & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
n=5 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
n=6 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

It shows that when two adjacent binomial coefficients in the triangle are added, the binomial coefficient in the next row between these two coefficients are produced.

All the above discussions are based on integers but in our next discussion we have highlighted those numbers which are of the form $\frac{u}{v}$ where $u, v \in \mathbb{Z}$. Here v must be nonzero, otherwise the division will not be possible. From the division of integers, there comes the concept of decimal numbers. For example $\frac{4}{5} = 0.8$.

Here we see that $\frac{2}{4} = 0.5$ ı.e. we can cancel common multiple from both numerator and denominator till their greatest common divisor will be 1.This extension of set of integers leads to the notion of rational numbers, denoted by $\mathbb{Q}$. Thus any number of the form $\frac{u}{v}$ where $u, v \in \mathbb{Z}$ with $v \neq 0$ and $\gcd(u, v) = 1$, is called rational number. Actually the symbol $\mathbb{Q}$ comes from the German word 'quotient 'which can be translated as 'ratio ', appeared in Bourbaki's Algebra(1998). Classical greek and Indian mathematicians studied theory of national numbers, as part of the general study of number theory. The concept of rational numbers were from the ancient times. Those can be expressed as a ratio of two different numbers that had no common divisors except 1. This prevalent concept which was there over a period of time was found to be inadequate, when in 500B.C. the Italian philosopher Hippasus proved the existence of irrational numbers. He was also a member of group of people who were called the Pythagorean mathematicians. His method of finding irrational numbers involve the technique of contradiction. There he had assumed that $\sqrt{2}$ is an irrational number. Then he moved on to show that no such rational number could exist. Therefore it should be something different. However, Pythagorus believed in the absoluteness of number and could not accept the existence of irrational numbers. So he sentenced Hippasus to death by drowning. In 16th century, finally Europeans accepted the existence of negative integers and fractional numbers. Thereby in 17th century, many mathematicians used decimal fractions with modern notations. Subsequently from 19th century onwards, the irrationals were seperated into algebraic and transcendental part. It had remained almost dormant since Euclid. Actually irrationals are closely associated to continued fractions, which had received attention at the hands of Euler.

Finally we end our discussions with the two fundamental theorems.

Theorem 1.0.5. *There $\nexists$ any $r \in \mathbb{Q}$ satisfying $r^2 = 2$.*

Proof. If possible, let $\exists\ r \in \mathbb{Q}$ such that $r^2 = 2$. Since $r \in \mathbb{Q}$, therefore it is of the form $\frac{x}{y}$ with $\gcd(x, y) = 1$ and $y \neq 0$. Hence $x^2 = 2y^2$. This proves x^2 is even and consequently x is also so. Suppose $x = 2k$. Then $4k^2 = 2y^2$ or $y^2 = 2k^2$. Hence y^2 is an even integer and so y is even. This shows $\gcd(x, y) \neq 1$, which ends up with contradiction. Thus for any rational quantity r, the equation $x^2 = 2$ has no solutions. Furthermore, this theorem leads us to the fact that $\sqrt{2}$ is irrational. □

Finally our next theorem indicates on the existence of irrational numbers.

Theorem 1.0.6. *Let k be a non-square positive integer. Then $\nexists$ any $r \in \mathbb{Q}$ such that $r^2 = k$.*

Proof. To the contrary, assume that $\exists$ a rational number r satisfying $r^2 = k$. Then r can be written as $\frac{a}{b}$ where $\gcd(a, b) = 1$. Then $a^2 = kb^2$ holds. For this positive integer k, there exists a positive integer l such that

$$\begin{aligned} & l^2 < k < (l+1)^2 \\ \Rightarrow\ & b^2 l^2 < a^2 < (l+1)^2 b^2 \\ \Rightarrow\ & bl < a < (l+1)b \\ \Rightarrow\ & 0 < a - bl < b. \end{aligned} \tag{1.0.1}$$

Further,

$$(kb - al)^2 = k^2b^2 - 2kbal + (al)^2 = k[a^2 - 2abl + (bl)^2] = k(a - bl)^2$$

So $k = \dfrac{(kb - al)^2}{(a - bl)^2}$. Since a and b are prime to each other and $\dfrac{a}{b}$, $\left(\dfrac{ka - al}{a - bl}\right)^2$ are two representation of k, therefore we have $a - bl > b$ and this contradicts (1.0.1). So this completes the proof. ☐

Finally we are at the edge of culminating our discussions related to propagation of numbers. In the concluding part, we conduct the study of real numbers which is the union of rationals and irrationals. The set of real numbers is denoted by $\mathbb{R}$. The creditability of uncovering $\mathbb{R}$ would not goes to a single person. The development took 2000 years and many renowned mathematicians had contributed with their important thoughts on $\mathbb{R}$. The notion of $\mathbb{R}$ had started its development from ancient Greece. Euclid had developed a theory of proportions which is equivalent to modern theory of real numbers. In 17th century, John Napier and Simon Stevin introduced the concept of infinite decimal expansion. Cantor and Dedekind had given their contributions to originate the modern theories of $\mathbb{R}$. In the following sections we are going to discuss few important properties of $\mathbb{R}$.

Order Properties of $\mathbb{R}$

The linear relation '$<$' on $\mathbb{R}$ defined by "$x < y$ if $x, y \in \mathbb{R}$ *i.e.* x is less than y". For the reals x, y, z, it satisfies the following properties:

1. Law of Trichotomy: $x < y$ or $y < x$ or $x = y$ holds.
2. If $x < y$ and $y < z$, then $x < z$.
3. If $x < y$, then $x + z < y + z$.
4. If $x < y$ and $z > 0$, then $xz < yz$.

The set $\mathbb{R}$ together with the ordered relation defined on it is said to be ordered set. For any $x \in \mathbb{R}$, the concept of absolute property of $\mathbb{R}$ is defined as

$$\begin{aligned} |x| &= x, \text{ if } x > 0 \\ &= 0, \text{ if } x = 0 \\ &= -x. \text{ if } x < 0. \end{aligned}$$

Completeness Properties of $\mathbb{R}$

Next we are going to discuss the completeness property of $\mathbb{R}$. The discussion starts with the following definition.

Definition 1.0.1. *Let $K \subset \mathbb{R}$. Then a real number u is said to be an upper bound(lower bound) of K if $x \in K$ and $x \leq u (x \geq u)$. If K has an upper bound(lower bound), then it is called bounded above(bounded below).*

Example 1.0.6. *Let $K = \{x \in \mathbb{R} : 3 < x < 4\}$. Note that K is bounded above and 4 is the upper bound. Also K is bounded below and 3 is the lower bound.*

The last example raises the question, whether the upper bound 4 and the lower bound 3 is greatest or least respectively. The following definition of least upper bound and greatest lower bound will be the answer to the raised question.

Definition 1.0.2. *Let $K \subset \mathbb{R}$. If K is bounded above(bounded below), then an upper bound (lower bound) is said to be the least upper bound(greatest lower bound) or supremum(infimum) if it is less(greater) than every upper(lower) bounds of K.*

Actually it is a deeper property of $\mathbb{R}$ that for any non-empty bounded above(below) subset of K of $\mathbb{R}$, the least upper bound(greatest lower bound) do exists. This property of $\mathbb{R}$ is called the supremum(infimum) property. Note that we can establish these two properties are equivalent and one implies other. Furthermore, the supremum property of $\mathbb{R}$ can be treated as an axiom, known to be the completeness property of $\mathbb{R}$. The statement is as follows:

Statement 1.0.1. *Axiom of least upper bound: If a set K is bounded above, then it has a least upper bound i.e. there exists a unique real number M satisfying*

1. *$x \leq M$, $\forall\, x \in K$.*
2. *for arbitrary $\epsilon (> 0)$, there exists an element $\alpha \in K$ such that $M - \epsilon < \alpha \leq M$.*

It is not necessary that every subset of $\mathbb{R}$ should have an upper bound. For instance it can be examined that $\mathbb{N}$ is not bounded above and thus it has no upper bound. Now taking help of the axiom of least upper bound, we are going to show the existence of greatest lower bound for a non–empty bounded below subset of $\mathbb{R}$.

Theorem 1.0.7. *A non-empty subset K of $\mathbb{R}$ which is bounded below, has the greatest lower bound i.e.there exists a unique real number m such that*

1. $x \geq m, \; \forall \, x \in K$.
2. *For arbitrary $\epsilon(> 0)$, there exists an element $\beta \in K$ such that $m \leq \beta < m + \epsilon$.*

Proof. Note that K is a non empty set, which is bounded below. Then $\exists \; k \in \mathbb{R}$ such that $x \geq k, \; \forall \, x \in K$. Consider $K' = \{-x : \; x \in K\}$. Let $y \in K'$. Then $-y \in K$ and $-y \geq K$ together implies $y \leq -k$. This is true for all $y \in K'$. This shows K' is bounded above. Then from least upper bound axiom, we obtain $M = \sup K'$. We need to show $-M = \inf K$. Let $t \in K$. Then $-t \in K'$ implies $-t \leq M$. Thus we have $t \geq -M$. Let $\epsilon(> 0)$ be chosen arbitrarily. Then $\alpha \in K'$ such that

$$M - \epsilon < \alpha \leq M \Rightarrow -M \leq -\alpha < -M + \epsilon.$$

Since $\alpha \in K'$, then $-\alpha = \beta \in K$ and thus taking $-M = m$ we have,

1. $x \geq m, \; \forall \, x \in K$.
2. for arbitrary $\epsilon(> 0)$, there exists an element $\beta \in K$ such that $m \leq \beta < m + \epsilon$.

□

Our next phase of discussion deals with the concept of functions between two arbitrary sets. The notion of function has an paramount importance not only in number theory. It helps to correlate between various algebraic structures. It is actually a rule of correspondence between the elements of two sets. The idea of function was developed in the seventeenth century. During this period mathematician Rene Descartes$(1596 - 1650)$ used it to describe many mathematical relationship in his book **Geometry**. The term **function** was introduced by Gottfried Wilhelm Leibnitz$(1646 - 1716)$, almost fifty years after the publication of Geometry. The idea was further formalized by Leonhard Euler$(1707-1783)$. However the present day conception of function is attributed to Dirichlet$(1805 - 1859)$, who in 1837 proposed the definition of a function as a rule of correspondence that assigns a unique value of an independent variable. Now a function from a set X to an another set Y can be defined as follows:

Definition 1.0.3. *For two non-empty sets X and Y, a relation f from X into Y is called a function from X into Y if*

1. *domain of f is set X*
2. *f is well-defined in the sense that for x_1, $x_2 \in X$ with $x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$.*

Actually f is a subset of $X \times Y$, where X is referred as domain of f, denoted by Dom(f), and the set Y is said to be co-domain of f. Here the set $f(X) = \{f(x) : x \in X\}$ is a subset of Y. This $f(X)$ is called range of f, denoted by Imf. For instance, consider $X = Y = \mathbb{R}$. Then $f(x) = 2x$, $\forall\, x \in \mathbb{R}$ is a function from $\mathbb{R}$ to $\mathbb{R}$ which is also called real valued function.

Moreover, there are few types of functions such as $f(x) = x \ \forall\, x \in X$ from X to X, called identity function and $f(x) = c$ for some constant c is known as constant function.

Two functions $f, g : X \to Y$ are said to be equal if $f(x) = g(x) \ \forall\, x \in X$. Sometimes functions can produce same values for different elements of domain set such as if we consider $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x|$, then we can see that $f(3) = f(-3)$ but $3 \neq -3$. From this, we have the following definition.

Definition 1.0.4. *A function $f : X \to Y$ is said to be injective when for every x_1, $x_2 \in X$ if*

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

Moreover, if for every $y \in Y$ there exists at least one $x \in x$ such that $f(x) = y$ holds then f is said to be surjective. Intuitively, a surjective map covers the whole of the codomain set i.e. Im(f) is the codomain of f. f is called bijective if it is both injective and surjective.

Suppose $A = \{1, 2, 3\}$ and $B = \{p, q, r, s, t\}$ and $f : A \to B$ be defined by

$$f(1) = p, f(2) = r, f(3) = s.$$

Since p, q, r have only one preimage and s, t have no preimage, therefore f is injective. On the other hand, suppose $A = \{1, 2, 3, 4, 5\}$ and $B = \{p, q, r\}$. Let $f : A \to B$ and $g : A \to B$ be respectively defined by

$$f(1) = q, f(2) = p, f(3) = q, f(4) = r, f(5) = p;$$
$$g(1) = r, g(2) = p, g(3) = p, g(4) = r, g(5) = r.$$

It is clear that f is surjective but g is not. Also, here f fails to be injective. Next let us consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 5x + 2$. Here f is an example of a bijective function.

Now consider a function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sin x^2$. Then we see that the function f is the amalgam of two functions $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = \sin x$ and $g(x) = x^2$. This originates the notion of composition of two functions.

Definition 1.0.5. *Consider two functions* $f : X \to Y$ *and* $g : Y \to Z$. *Then the composition of* f *and* g, *denoted as* $g \circ f$, *is defined as* $(g \circ f)(x) = g(f(x))$ *where* $g \circ f : X \to Z$.

Finally, we end this session of discussion by the concept of inverse of a function.

Definition 1.0.6. *Let* $f : X \to Y$ *be a bijective function. Then the function* $f^{-1} : Y \to X$ *is said to be inverse of* f. *The domain of the inverse function* f^{-1} *is the range of* f *and the range of* f^{-1} *is the domain of* f.

The concluding part of the chapter deals with the study of a special type of real-valued function whose domain set is, in particular, a set of naturals *i.e.*$f : \mathbb{N} \to \mathbb{R}$, denoted by $f(n) = x_n$ where $n \in \mathbb{N}$ and $x_n \in \mathbb{R}$. In other words, it can be interpreted as $1 \mapsto x_1$, $2 \mapsto x_2, \ldots$ and so on. Therefore, the representation x_n prevails. The set $\{x_n : n \in \mathbb{N}\}$ is a subset of $\mathbb{R}$ which is said to be the range of the sequence. For example, let us consider a function $f : \mathbb{N} \to \mathbb{R}$ defined as $f(n) = \frac{n}{n+1}$, $\forall\ n \in \mathbb{N}$. Here the sequence is $\{\frac{n}{n+1}\}_n$, also denoted as $\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots\}$. The range set of this sequence is $\{\frac{n}{n+1} : n \in \mathbb{N}\}$. Now we are going to discuss the boundedness of sequence, whose definition is as follows:

Definition 1.0.7. *A sequence is said to be bounded above or bounded below according as the range set of the sequence is bounded above or below. It follows that the sequence* $\{x_n\}$ *is bounded above(below) if there exists a real quantity* $G(g)$ *such that* $x_n \leq G(x_n \geq g)$ $\forall\ n \in \mathbb{N}$ *and* $G(g)$ *is called the upper(lower) bound of the sequence. A sequence is said to be bounded if it is both bounded above and bounded below.*

From the last example, we can see that $x_n = \dfrac{n}{n+1} = 1 - \dfrac{1}{n+1} \leq 1$. Thus $\{x_n\}$ is bounded above and 1 is the upper bound. Consider $\{\frac{1}{n}\}$ for all $n \in \mathbb{N}$, where the values of the range set goes to zero if $n \to \infty$. In other words, for all large values of n, the values of the range set cluster near *zero*. This generates the concept of convergence of a sequence.

Definition 1.0.8. *A real number l is defined as the limit of a sequence $\{x_n\}$ if for any arbitrary $\epsilon(>0)$, $\exists\, m \in \mathbb{N}$ such that*

$$|x_n - l| < \epsilon, \ \forall\, n \geq m.$$

In this case, the sequence is said to be convergent and can be written as $\lim_{n\to\infty} x_n = l$.

The question arises: Is the limit l of the convergent sequence is unique? We are fortunate enough to have the following theorem as the answer to the question.

Theorem 1.0.8. *Limit of a convergent sequence is unique.*

Proof. Let the sequence $\{x_n\}$ converges to l and l'. Then for a pre-assigned $\epsilon(>0)$, $\exists\, m_1, m_2 \in \mathbb{N}$ such that

$$|x_n - l| < \frac{\epsilon}{2}, \ \forall\, n \geq m_1,$$

and

$$|x_n - l'| < \frac{\epsilon}{2}, \ \forall\, n \geq m_2.$$

Let $m = \max\{m_1, m_2\}$. Then,

$$\begin{aligned} |l - l'| &= |(x_n - l) - (x_n - l)| \\ &\leq |(x_n - l') - (x_n - l)| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \ \forall\, n > m. \end{aligned}$$

Since $\epsilon(>0)$ is arbitrary, therefore the uniqueness follows. ☐

The discussion of the following theorem is based on the connection between convergence and boundedness.

Theorem 1.0.9. *A convergent sequence is bounded.*

Proof. Let the sequence $\{x_n\}$ converges to l. Then for a pre-assigned $\epsilon(>0)$, $\exists\, m$ such that

$$|x_n - l| < \epsilon, \ \forall\, n \geq m, \textit{i.e. } l - \epsilon < x_n < l + \epsilon, \ \forall\, n \geq m.$$

If A and B be the greatest and least of the finite set $\{x_1, x_2, \ldots, x_n, \ldots, l-\epsilon, l+\epsilon\}$, then $B \leq x_n \leq A \ \forall\, n$. Hence the sequence $\{x_n\}$ is bounded. ☐

Note that the converse of the above theorem is not true in general. For instance, consider the sequence $\{(-1)^n\}$ which is bounded but not convergent. So, if a sequence does not converge then two possibilities may arise. Either the sequence diverge or oscillates.

Definition 1.0.9. *A sequence $\{x_n\}$ is said to be divergent and diverges to $+\infty$, if for an arbitrary positive real number N, however large it is, $\exists\ m \in \mathbb{N}$ such that*

$$x_n > N,\ \forall\ n \geq m.$$

Also, the sequence $\{x_n\}$ is said to be divergent and diverges to $-\infty$, if for an arbitrary positive real number N, however large it is, $\exists\ m \in \mathbb{N}$ such that

$$x_n < -N,\ \forall\ n \geq m.$$

Finally, a sequence which is neither convergent nor divergent is said to be oscillatory sequence. For example, the sequence $\{2^n\}$ diverges to $+\infty$ and the sequence $\{-n^2\}$ diverges to $-\infty$. The sequence $\{(-1)^n\}$ is an oscillatory one.

Finally, we close this discussion with monotone sequence and few properties related to it.

Definition 1.0.10. *A sequence $\{x_n\}$ is said to be monotone increasing(decreasing) sequence if $x_{n+1} \geq (\leq) n,\ \forall\ n \in \mathbb{N}$.*

As an example, let us consider the sequence n^2 *i.e.*$\{1, 4, 9, \ldots\}$. This sequence is monotone increasing, however the sequence $\{\frac{1}{2^n}\}$ *i.e.*$\{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots\}$ is monotone decreasing.

Theorem 1.0.10. *A monotone increasing sequence, if bounded above, is convergent and converges to least upper bound.*

Proof. Let $\{x_n\}$ be the monotone increasing sequence, bounded above. Then for a pre-assigned $\epsilon(> 0)$, $\exists\ r \in \mathbb{N}$ such that

$$M - \epsilon < x_r \leq M < M + \epsilon.$$

Here M is the least upper bound of $\{x_n\}$. Therefore, $M - \epsilon < x_r \leq M + \epsilon$. Again, since $\{x_n\}$ is monotone increasing then for $n \geq r$ we find $x_n \geq x_r$. Thus, $M - \epsilon < x_r < x_n \leq M < M + \epsilon \Rightarrow |x_n - M| < \epsilon\ \forall\ n \geq r$. This completes the proof.

□

Remark 1.0.2. *A monotone increasing sequence, if unbounded above, is divergent and diverges to $+\infty$.*

Analogously, we can state that

Theorem 1.0.11. *A monotone decreasing sequence, if bounded below, is convergent and converges to greatest lower bound.*

Remark 1.0.3. *A monotone decreasing sequence, if unbounded below, is divergent and diverges to $-\infty$.*

Exercises:

1. Using Mathematical induction show that $1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$, for all positive integers n.
2. Using induction on n prove the identity $n^2 < n!$ for all integers $n \geq 4$.
3. What is the coefficient of x^7 in $(3x + 2)^{19}$?
4. Find the coefficient of x^5y^7 in $(x + y)^{10}$.
5. Suppose S is a set of $n+1$ integers. Prove that there exist distinct $a, b \in S$ such that $a - b$ is a multiple of n.
6. Show that in any group of n people, there are two who have an identical number of friends within the group.
7. Determine whether the function $f : \mathbb{Z} \to \mathbb{Q}$ defined by $f(x) = 2^x$, for all $x \in \mathbb{R}$ is bijective or not.
8. Let $f, g : \mathbb{R} \to \mathbb{R}$ be two functions, given by $f(x) = |x| + x$ for all $x \in \mathbb{R}$ and $g(x) = |x| - x$ for all $x \in \mathbb{R}$. Evaluate $f \circ g$ and $g \circ f$.
9. A sequence $\{x_n\}$ is defined by $x_n = \sqrt{5}$ and $x_{n+1} = \sqrt{5x_n}$ for $n \geq 1$. Prove that $\lim x_n = 5$.
10. Show the convergence of the sequence $\{(1 + \frac{1}{n})^n\}$.

2

Theory of Divisibility

> *"A marveilous newtrality have these things mathematicall, and also a strange participation between things supernaturall, immortall, intellectuall, simple and indivisible, and things naturall, mortall, sensible, componded and divisible."*
>
> – John Dee

2.1 Introduction

Mathematics is the Universe's natural tongue. From very beginning of our existence as a species, numbers have deeply mesmerised us. Due to Carl Friedrich Gauss "Number theory is one of the oldest branches of Mathematics which established a relationship between numbers belonging to the set of real numbers".

The pureness of Number Theory has charmed mathematicians generation after generation — each contributing to the branch that Carl Gauss described as the "Queen of Mathematics." Today, however, a basic understanding of Number Theory is an absolute precursor to cutting-edge software engineering, specifically security-based software. Number Theory is at the heart of cryptography — which is itself experiencing a engrossing period of rapid evolution, ranging from the famous RSA algorithm to the wildly-popular blockchain world.

Two clear-cut moments in history stand out as curvature points in the development of Number Theory. First, in archaic times, Euclid put forth his GCD (Greatest Common Divisor) algorithm — a splendid set of steps that simplifies fractions to their simplest form using geometrical observations. Then, approximately two-thousand years later, Gauss formalized Euclid's principles by combining Euclid's informal writings with his own extensive proofs in the timeless Disquistiones Arithmeticae.

2.2 Divisibility

When an integer is divided by a second integer($\neq 0$), the quotient may or may not be an integer. For instance, $36/6 = 6$ is an integer, while $18/7 = 2.5$ is not. This observation leads to the following definition.

Definition 2.2.1. *If a and b are integers, we say that b is divisible by $a(\neq 0)$ if there exists an integer c such that $b = ac$. Also, we say that a is a divisor or factor of b, denoted by $a|b$. If a does not divides b, then we write $a \nmid b$.*

Example 2.2.1. 10 *is divisible by* 5 *because there exist an integer* 2 *such that* $10 = 5 \times 2$. *We say* $5|10$.

Proposition 2.2.1. *For any integers a, b, c, d the following statements are true:*

1. $a|0, 1|a, a|a.$
2. $a|b \Rightarrow ca|cb, \forall c \in \mathbb{Z}.$
3. $a|b$ *and* $b|c \Rightarrow a|c.$
4. $a|b$ *and* $b|a \Rightarrow a = \pm b.$
5. $a|b$ *and* $a|c \Rightarrow a|(bx + cy)$ *for arbitrary integers x and y.*

Proof. 1. Obvious.

2. Here,

$$\begin{aligned} a|b &\Rightarrow b = da \text{ for some integer } d, \\ &\Rightarrow cb = d(ca) \\ &\Rightarrow ca|cb. \end{aligned}$$

3. Here, $a|b \Rightarrow b = aq$ and $c|d \Rightarrow d = cp$ for some integers p and q. Therefore $c = a(pq)$. Hence $bd = ac(pq)$. Therefore $ac|bd$, as pq is an integer.

4. Here, $a|b \Rightarrow b = ap$ for some integer p. Also, $b|c \Rightarrow c = bq$ for some integer q. Therefore $c = bq = a(pq)$. Therefore $a|c$.

5. Here, $a|b \Rightarrow b = ap$ for some integer p. Therefore $b = bpq$. Also, $b|a \Rightarrow a = bq$ for some integer q implies $pq = 1$. As p, q are integers either, $p = q = 1$ or $p = q = -1$. Therefore $a = \pm b$.

6. Here, $a|b \Rightarrow b = ap$ for some integer p and Here, $a|c \Rightarrow b = aq$ for some integer q. Therefore $bx + cy = apx + aqy = a(px + qy)$. Now, $px + qy \in \mathbb{Z}$ as $p, q, x, y \in \mathbb{Z}$. Therefore $a|(bx + cy)$.

□

Theorem 2.2.1. *The Division Algorithm: Given any two integers* a *and* b*, with* $b > 0$ *there exists unique integers* q *and* r *such that* $a = bq + r$ *with* $0 \leq r < b$.

Proof. Let a and b be two fixed integers with $b \neq 0$. Let $A = \{n \in \mathbb{N}|n = a - by, y \in \mathbb{Z}\}$. Our claim is $A \neq \phi$. For this there are two possibilities viz:

1. If $a \geq 0$, then $a - b(0) = a \geq 0$. So $a - by$ is non–negative for $y = 0(a \geq 0)$.

2. If $a < 0$, then $-a > 0$. Since, b is a positive integer, we must have $b \geq 1$. Multiplying the inequality by a positive quantity gives, $(-a)b \geq (-a)$ implies $a - ab \geq 0$. So $a - by$ is non–negative for $y = a(< 0)$. Hence $A \neq \phi$.

Since, $A \subset \mathbb{N}$, by well ordering principle A has a least element say r. Since, $s \in A$, therefore, $r = a - by$ for some $y = q$. Thus we found integers r and q such that $r = a - bq$ or $a = r + bq$. Since, $r \in A$, therefore $r \geq 0$. Next our claim is $r < b$. On the contrary, if we assume $r \geq b$, then $0 \leq r - b = (a - bq) - b = a - b(q + 1) < r$, which leads to a contradiction as r is the least in A. Hence $r < b$. Thus we found two integers q and r such that $a = bq + r$ with $0 \leq r < b$.

The last part of the proof deals with the uniqueness of q and r with the above properties. If possible, let there be two pair of integers r_1, q_1 and r_2, q_2 satisfying

$$r_1 + bq_1 = a = r_2 + bq_2 \tag{2.2.1}$$

with

$$0 \leq r_1 \leq b \text{ and } 0 \leq r_2. \tag{2.2.2}$$

We need to prove $r_1 = r_2$ and $q_1 = q_2$.

If $r_1 \leq r_2$, then 2.2.1 shows

$$b(q_1 - q_2) = r_2 - r_1. \tag{2.2.3}$$

Since by hypothesis, $b > 0, r_2 \geq r_1$, therefore $q_1 - q_2$ must be a non negative integer. Hence $r_2 - r_1$ must be one of $0, b, 2b, 3b, \ldots$. But $0 \leq r_2 \leq r_1 \leq b$ implies $r_2 - r_1 = 0$. Hence by 2.2.3 and the preceeding equation together with the hypothesis $b > 0$, we have $q_1 = q_2$. Similarly, taking $r_1 \geq r_2$, proves the uniqueness of q and r. □

For another proof we give explicit formulae for the quotient and remainder in terms of the greatest integer function, which will be done in the consequent chapter of the book.

Remark 2.2.1. *1. When* $b \nmid a, r$ *satisfies strong inequality* $0 < r < b$.

2. Here q *and* r *called quotient and remainder.*

3. bq *is largest multiple of* b *which does not exceed* a.

Example 2.2.2. *Suppose we are dividing* 51 *by* 5 *then,* $51 = 5 \times 10 + 1$. *Comparing with the theorem we get,* $a = 51, b = 5, q = 10, r = 1$.*Here* $q = 10$ *is the quotient and* $r = 1$ *is remainder.*

Corollary 2.2.1. *If* a, b *be two integers with* $b > 0$*, then there exists integers* Q *and* R *such that* $a = bQ \pm R,\ \ 0 \leq R < \dfrac{b}{2}$.

Proof. From Division algorithm we have, for any two integers a and b with $b > 0$, there exists unique integers q and r such that

$$a = bq + r,\ 0 \leq r < b \tag{2.2.4}$$

We now consider three following cases: Case(i): Let $r < \frac{b}{2}$ and taking $q = Q$ and $r = R$ in equation (2.2.4), we have

$$a = bQ + R, 0 \leq R < \frac{b}{2}$$

Case(ii): Let $r > \frac{b}{2}$, then from equation(2.2.4)

$$\begin{aligned} a &= bq + r \\ &= b(q+1) + (r - b) \\ &= b(q+1) - (b - r). \end{aligned}$$

Taking $q+1 = Q$ and $b-r = R$, we have $a = bQ-R$ where $R = b-r < b-\frac{b}{2} = \frac{b}{2}$. Therefore $a = bQ - R,\ 0 \leq R < \frac{b}{2}$. Now combining case (i) and (ii) we have,

$$a = bQ \pm R,\ 0 \leq R < \frac{b}{2}$$

Case(iii): Let $r = \frac{b}{2}$, then from equation(2.2.4)

$$a = bQ + R,\ \text{where } q = Q\ \text{ and } r = R = \frac{b}{2}$$

Again from the equation(2.2.4) we have,

$$a = bq + r = b(q+1) - (b - r) = bQ + R$$

where $q + 1 = Q$ and $-(b - r) = R$ that is $R = -b + \frac{b}{2} = -\frac{b}{2}$. Which shows that Q and R is not unique in this case thus case(iii) is not possible. ☐

Remark 2.2.2. *(i) Here in the above proof Q and R are unique except when $R = \frac{b}{2}$. In this case that is for $R = \frac{b}{2}$, R is called minimal remainder or the absolutely least remainder of a with respect to b.*
(ii) When $r < \frac{b}{2}$, the minimal remainder is $R = r$.
(iii) When $r > \frac{b}{2}$, the minimal remainder is $R = r - b$.

Here we have done an illustration of the concept minimal remainder by an example. Let us choose $a = 51$ and $b = 6$ then $51 = 6 \times 8 + 3$(of the form $a = bQ + R,\ Q = 8,\ R = 3$). Also we can write $51 = 6 \times 9 - 3$(of the form $a = bQ - R,\ Q = 9,\ R = 3$). Thus Q and R are not unique as $R = \frac{b}{2} = 3$. Which is case (iii) of above corollary.
Now if we choose $a = 50$ and $b = 6$ then $50 = 6 \times 8 + 2$. Thus in this case $r = 2 < \frac{b}{2} = 3$ and the minimal remainder is $R = 2$. Which is case (i) of above corollary.
Now if we choose $a = 52$ and $b = 6$ then $52 = 6 \times 8 + 4$. Thus in this case $r = 4 > \frac{b}{2} = 3$ and the minimal remainder is $R = r - b = 4 - 6 = -2$. Which is case (ii) of above corollary.

Theorem 2.2.2. *Prove that every integer is of the form,*

1. $3k$ *or* $3k \pm 1$.
2. $4k$ *or* $4k \pm 1$ *or* $4k \pm 2$.
3. $5k$ *or* $5k \pm 1$ *or* $5k \pm 2$.
4. $6k$ *or* $6k \pm 1$ *or* $6k \pm 2$ *or* $6k \pm 3$.

Proof. From the above corollary any integer a is of the form

$$a = bk \pm r \text{ where } b, k, r \in \mathbb{Z} \text{ and } 0 \leq |r| \leq \frac{b}{2}. \tag{2.2.5}$$

1. When $b = 3$, we get from 2.2.5 $a = 3k \pm r$ where $0 \leq |r| \leq \dfrac{3}{2} = 1.5$. Therefore $r = 0, \pm 1$.
2. When $b = 4$ we get from 2.2.5, $a = 4k \pm r, 0 \leq |r| \leq \dfrac{4}{2} = 2$, i.e. $r = 0, \pm 1, \pm 2$. Therefore $a = 4k, 4k \pm 1, 4k \pm 2$.
3. Rests treated as exercises.

□

2.3 Worked out Exercises

Problem 2.3.1. *For any two integers* a *and* b *with* $b > 0$*, there exists unique integers* q_1 *and* r_1 *such that* $a = bq_1 + cr_1$ *where* $0 \leq r_1 < \dfrac{b}{2}, c = \pm 1$.

Solution 2.3.1. *By division algorithm we have* $a = bq + cr, 0 \leq r < b$.

Case I $r < \dfrac{b}{2}$, *take* $q_1 = q, c = 1, r_1 = r$. *Therefore* $a = bq_1 + cr_1, 0 \leq r_1 < \frac{b}{2}, c = \pm 1$.

Case II $r > \frac{b}{2}$, *therefore* $0 < b - r < \frac{b}{2}$ *take* $q_1 = q_0 + 1, r_1 = b - r$ *and* $c^2 = -1$, *therefore,* $a = bq_1 + cr_1$ *where* $0 \leq r_1 < \frac{b}{2}, c = -1$.

Case III $r = \frac{b}{2}$ *then* $q_1 = q, c = 1, r_1 = r$. *Therefore* $a = bq_1 + cr_1, r_1 = \dfrac{b}{2}, c = 1$ *and if* $q_1 = q + 1, r_1 = b - r$ *and* $c = -1$. *Therefore* $a = b(q+1) - (b - r) = bq_1 + cr_1, \dfrac{b}{2} = r, c = -1$. *In this case* q_1 *and* r_1 *is not unique, so* $a = bq_1 + cr_1, 0 \leq r_1 < \frac{b}{2}, c = \pm 1$.

Problem 2.3.2. *Show that every square integer is of the form* $5k$ *or* $5k \pm 1$ *for some* $k \in \mathbb{Z}$.

Solution 2.3.2. *Note that every integer is of the form* $5p, 5p \pm 1, 5p \pm 2$ *for some* $p \in \mathbb{Z}$. *Square of these numbers are of the form:*

$$\begin{aligned}
(5p)^2 &= 5 \times 5p^2 = 5k, \textit{where } k = 5p^2 \textit{ is a positive integer} \\
(5p \pm 1)^2 &= 25p^2 \pm 10p + 1 = 5(5p^2 \pm 2p) + 1 = 5k + 1, \textit{where } k = 5p^2 \pm 2p + 1 \in \mathbb{Z} \\
(5p \pm 2)^2 &= 25p^2 \pm 20p + 4 \\
&= 5(5p^2 \pm 4p + 1) - 1 \\
&= 5k - 1, \textit{where } k = 5p^2 \pm 4p + 1 \in \mathbb{Z}.
\end{aligned}$$

Problem 2.3.3. *Show that cube of any integer is of the form* $9p, 9p + 1, 9p + 8$*(or* $9p, 9p \pm 1$*).*

Solution 2.3.3. *Here,*

$$\begin{aligned}
(3m)^3 &= 27m^3 = 9p, \ \textit{where } p = 3m^3 \in \mathbb{Z} \\
(3m+1)^3 &= 27m^3 + 27m^2 + 9m + 1 \\
&= 9(3m^3 + 3m^2 + m) + 1 \\
&= 9p + 1, \ \textit{where } p = 3m^3 + 3m^2 + m \in \mathbb{Z} \\
(3m-1)^3 &= 27m^3 - 27m^2 + 9m - 9 + 8 \\
&= 9(3m^3 - 3m^2 + m - 1) + 8 \\
&= 9p + 8, \ \textit{where } p = 3m^3 - 3m^2 + m - 1 \in \mathbb{Z} \\
\textit{Also}, \ (3m-1)^3 &= 9(3m^3 - 3m^2 + m) - 1 \\
&= 9p - 1, \ \textit{where } p = 3m^3 - 3m^2 + m \in \mathbb{Z}.
\end{aligned}$$

Problem 2.3.4. *Prove that the expression* $\dfrac{a(a^2+2)}{3}$ *is an integer for* $a \geq 1$.

Solution 2.3.4. *Applying Division Algorithm, any integer* a *can be expressed in the form* $3q, 3q+1, 3q+2$. *Taking* $a = 3q$ *we obtain* $\frac{a(a^2+2)}{3} = q(9q^2+2)$, *an integer. Similarly putting* $a = 3q+1$ *and* $a = 3q+2$ *we obtain* $(3q+1)(3q^2+2q+1)$ *and* $(3q+2)(3q^2+4q+2)$ *respectively, both of which are integers. Hence the result is proved.*

Problem 2.3.5. *Show that one of every three consecutive integer is divisible by* 3.

Solution 2.3.5. *Let* $a, a+1, a+2$ *be any three consecutive integers, then* a *is of the form* $3p, 3p+1, 3p-1$ *where* $p \in \mathbb{Z}$. *If* $a = 3p$, *then* a *is divisible by* 3. *If* $a = 3p+1$, *then* $a + 2 = 3p + 3 = 3(p+1)$ *is divisible by* 3. *If* $a = 3p - 1$, *then* $a + 1 = 3p + 1 - 1 = 3p$ *is divisible by* 3.

Problem 2.3.6. *Find the minimal remainder of* 416 *with respect to (i)* 37 *(ii)* 42.

Solution 2.3.6. **(i)** *Here* $a = 416, b = 37$. *Therefore* $416 = 37 \times 11 + 9$ *(Why!). Therefore the minimal remainder is* $R = 9$.

(ii) *Left to the reader.*

Problem 2.3.7. *Show that* $a^{n+1} - (a-1)n - a$ *is divisible by* $(a-1)^2, a$ *being an integer.*

Solution 2.3.7. *Since* $a \in \mathbb{Z}$*, we have*

$$\begin{aligned} a^{n+1} - (a-1)n - a &= a(a^n - 1) - (a-1)n \\ &= a(a - 1\{a(a^{n-1} + \cdots + 1\ ) \ - n\}) \\ &= (\ a - 1)\{(a^n + a^{n-1} + \cdots + a) - n\} \\ &= (\ a - 1)^2\{(a^{n-1} + a^{n-2} + \cdots + 1\ ) + (\ a^{n-2} + \cdots + 1\ ) + \cdots + 1\ \}. \end{aligned}$$

The given expression is divisible by $(a-1)^2$*.*

Problem 2.3.8. *If both* a *and* b *are odd positive integers then* $a^4 + b^4 - 2$ *is divisible by* 8*.*

Solution 2.3.8. *Let* $a = 2n_1 + 1$ *and* $b = 2n_2 + 1$ *be the odd positive integers, where* n_1, n_2 *are positive integers. Thus we have,*

$$\begin{aligned} &(2n_1 + 1)^4 + (2n_2 + 1)^4 - 2 \\ &= (2n_1)^4 + 4 \cdot (2n_1)^3 + 6 \cdot (2n_1)^2 + 4 \cdot (2n_1) + 1 + (2n_2)^4 + 4 \cdot (2n_2)^3 + 6 \cdot (2n_2)^2 \\ &+ 4 \cdot (2n_2) + 1 - 2 \\ &= 16(n_1^4 + n_2^4) + 16(n_1^3 + n_2^3) + 24(n_1^2 + n_2^2) + 8(n_1 + n_2) \\ &= 8[2(n_1^4 + n_2^4) + 2(n_1^3 + n_2^3) + 3(n_1^2 + n_2^2) + (n_1 + n_2)]. \end{aligned}$$

Problem 2.3.9. *Show that the product of two integers of the form* $4n + 1$ *is again of this form, while the product of two integers of the form* $4n + 3$ *is of the form* $4k + 1$*.*

Solution 2.3.9. *Product of two integers of the form* $4n + 1$ *gives us* $(4n + 1)(4m + 1) = 4(4mn + m + n) + 1 = 4k + 1, k \in \mathbb{Z}$*. Similarly* $(4n + 3)(4m + 3) = 4(4mn + 3m + 3n + 2) + 1 = 4k + 1, k \in \mathbb{Z}$*.*

Problem 2.3.10. *Show that the square of every odd integer is of the form* $8k+1$*.*

Solution 2.3.10. *Let* a *be an odd integer. Then* $n = 2s + 1$*,* s *being an integer. Now,* $a^2 = 4s(s + 1) + 1$*. If* s *is even, then* $s = 2m, m$ *being an integer. Hence*

$$a^2 = 8m(2m + 1) + 1 = 8k + 1, k = 2m + 1 \in \mathbb{Z}.$$

If s *is odd, then* $s = 2m + 1$*. It follows,*

$$a^2 = 8(2m + 1)(m + 1) + 1 = 8k + 1, k = (2m + 1)(m + 1) \in \mathbb{Z}.$$

Problem 2.3.11. *Let* m *be a positive integer. We define*

$$T(m) = \begin{cases} \frac{m}{2}, & \text{if } m \text{ is even;} \\ \frac{3m+1}{2}, & \text{if } m \text{ is odd.} \end{cases}$$

We, then form the sequence obtained by iterating T; $m, T(m), T(T(m)), T(T(T(m))), \ldots.$ *For instance, starting with* $m = 7$ *we have* $7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1, 2, 1, 2, 1, \ldots.$ A*well-known conjecture, sometimes called the* ***Collatz conjecture,*** ***asserts that*** *the sequence obtained by iterating* T *always reaches the integer* 1 *no* ***matter which*** *positive integer* m *begins the sequence.*

Show that the sequence obtained by iterating T *starting with* $m = \dfrac{2^{k-1}}{3}$, *where* k *is an even positive integer,* $k > 1$, *always reaches the integer* 1.

Solution 2.3.11. *If* $3m$ *is odd, then so is* m. *So* $T(m) = \frac{3m+1}{2} = \frac{2^{2k}}{2} = 2^{2k-1}$. *Since* $T(m)$ *is a power of* 2, *the exponent will decrease down to* 1 *with repeated iterations of* T.

Problem 2.3.12. *Show that if* a *is an integer, then* 3 *divides* $a^3 - a$.

Solution 2.3.12. *Here* $a^3 - a = a(a-1)(a+1)$. *Applying division Algorithm we have* $a = 3k, a = 3k+1$ *or* $a = 3k+2$, k *being an integer. If* $a = 3k$ *and* $a = 3k+1$, *then* $3|a$ *and* $3|(a-1)$ *respectively. Finally, if* $a = 3k+2$ *i.e.* $a+1 = 3(k+1)$, *then* $3|(a+1)$. *Combining, it shows* $3|a(a-1)(a+1) = a^3 - a$.

2.4 Greatest Common Divisor

If c and d be two arbitrary integers, not simultaneously zero, then the set of common divisors of c and d is a finite set of integers, always containing the integers $+1$ and -1(hence, their set of common divisors is non-null). Now every integer divides zero, so that if $c = d = 0$, then every integer serves as a common divisor of c and d. In this case, the set of common divisors of c and d turns to be infinite. In this article, we are interested on the greatest integer among the common divisors of two integers.

Definition 2.4.1. *The greatest common divisor of two integers* c *and* d, *that are not both zero, is the greatest integer which divides both* c *and* d.

In other words, the above definition can be formulated as

Definition 2.4.2. *If* c *and* d *be two arbitrary integers, not simultaneously zero, the greatest common divisor of* c *and* d *is the common divisor* e *satisfying the following:*

1. $e|a$ *and* $e|b$.
2. *If* $f|a$ *and* $f|b$ *then* $e \geq f$.

The greatest common divisor of c and d is written as (c, d) or $\gcd(c, d)$.

Example 2.4.1. *The common divisors of* 20 *and* 80 *are* $\pm1, \pm2, \pm4, \pm5, \pm10 and \pm 20$. *Hence* $\gcd(20, 80) = 20$. *Similarly, looking at sets of common divisors, we find that* $(12, 18) = 6, (50, 5) = 5, (19, 24) = 1, (0, 56) = 56, (-8, -16) = 8$, *and* $(-19, 361) = 19$.

We can also define the greatest common divisor of more than two integers.

Definition 2.4.3. *Let* $c_1, c_2, \dots, c_n$ *be integers, that are not all zero. The greatest common divisor of these integers is the greatest integer which is a common divisor of all of the integers in the set. The greatest common divisor of* $c_1, c_2, \dots, c_n$ *is denoted by* $(c_1, c_2, \dots, c_n)$ *or* $\gcd(c_1, c_2, \dots, c_n)$.

Example 2.4.2. *We see that* $(12, 18, 30) = 6$ *and* $(10, 15, 25) = 5$.

The following proposition can be used to find the greatest common divisor of a set of more than two integers.

Proposition 2.4.1. *If* $c_1, c_2, \dots, c_n$ *are integers, not simultaneously zero, then*

$$\gcd(c_1, c_2, \dots, c_n) = \gcd\big(c_1, c_2, \dots, (c_{n-1}, c_n)\big).$$

Before proceeding for proof, let us explain the proposition with an example: To find the greatest common divisor of the three integers $105, 140$, and 350, we see that $\gcd(105, 140, 350) = \gcd\big(105, (140, 350)\big) = \gcd(105, 70) = 35$.

Proof. In particular, a common divisor of the n integers $c_1, c_2, \dots, c_n$ is a divisor of c_{n-1} and c_n and therefore, a divisor of (c_{n-1}, c_n). Also, any common divisor of the $n-2$ integers $c_1, c_2, \dots, c_{n-2}$ and (c_{n-1}, c_n), must be a common divisor of all n integers, for if it divides (c_{n-1}, c_n), it must divide both c_{n-1} and c_n. Since the set of n integers and the set of the first $n-2$ integers together with the greatest common divisor of the last two integers have exactly the same divisors, their greatest common divisors are equal. ☐

Next we are particularly interested in pair of integers sharing no common divisors other than 1. Such pair of integers are said to be relatively prime or coprime.

Definition 2.4.4. *The integers* c *and* d, *not simultaneously zero, are said to be relatively prime(or coprime) if* c *and* d *have greatest common divisor* $(a, b) = 1$.

Example 2.4.3. *Since,* $\gcd(12, 13) = 1$ *therefore* $12, 13$ *are relatively prime.*

We can also define the relatively prime of more than two integers.

Definition 2.4.5. *We say that the integers* $c_1, c_2, \ldots, c_n$ *are mutually relatively prime(or coprime) if* $\gcd(c_1, c_2, \ldots, c_n) = 1$*. These integers are called pairwise relatively prime if for each pair of integers* c_i, c_j *from the set,* $\gcd(c_i, c_j) = 1$*, i.e., if each pair of integers from the set is relatively prime.*

If integers are pairwise relatively prime, they must be mutually relatively prime(Verify!). However, the converse fails is shown from the following example:

Example 2.4.4. *Consider the integers* $15, 21$*, and* 35*. Since* $(35, 55, 77) = (35, (55, 77)) = (35, 11) = 1$*, we see that the three integers are mutually relatively prime. However, they are not pairwise relatively prime, because* $(35, 55) = 5, (35, 77) = 7$ *and* $(55, 77) = 11$*.*

Remark 2.4.1. *Since the divisors of* $-a$ *are the same as the divisors of* a*, it follows that* $\gcd(a, b) = (|a|, |b|)$ *(where* $|a|$ *denotes the absolute value of* a *which equals* a *if* $a > 0$*, equals* $-a$ *if* $a < 0$*) and equals* 0 *if* $a = 0$*. Hence we can restrict our attention to greatest common divisors of pairs of positive integers.*

We will show that the greatest common divisor of the integers c and d, not simultaneously zero, can be written as a sum of multiples of c and d. To phrase this more lucidly, we use the following definition:

Definition 2.4.6. *If* c *and* d *are integers, then a linear combination of* c *and* d *is a sum of the form* $mc + nd$*, where both* m *and* n *are integers.*

The following theorem relates definition 2.4.6 and greatest common divisors.

Theorem 2.4.1. *The greatest common divisor of the integers* c *and* d*, not simultaneously zero, is the least positive integer that is a linear combination of* c *and* d*.(In other words, given integers* c *and* d*, not both of which are zero, there exist integers* m, n *such that* $\gcd(c, d) = mc + nd$*.)*

Before proceeding for the proof, let us illustrate the theorem succinctly with an example:

Example 2.4.5. *Consider the case in which* $c = 4$ *and* $d = 12$*. Here, the set* S *becomes* $S = \{4(-2) + 12 \cdot 1, 4(-1) + 12 \cdot 1, 4 \cdot 0 + 152 \cdot 1, \ldots\} = \{4, 8, 12, \ldots\}$*. Here* 4 *is the smallest integer in* S*, whence* $4 = \gcd(4, 12)$*.*

Proof. Let e be the least positive integer such that $e = ma + nb$ holds, m, n being integers.(Using the well-ordering property, there exist such least positive integer, also at least one of two linear combinations $1 \cdot c + 0 \cdot d$ and $(-1) \cdot c + 0 \cdot b$, where $c \neq 0$ is positive, do exist).

Claim(i) $e|c$ and $e|d$.

Claim(ii) $e = \gcd(c, d)$.

To fulfill Claim(i), applying Division Algorithm, we have $c = eq+r$ with $0 \leq r < e$. Now combining $e = ma + nb$ and $c = eq + r$, we obtain $r = (l - qm)c - qnd$. This shows that the integer r is a linear combination of c and d. Since $0 \leq r < e$, and e is the least positive linear combination of c and d, we conclude that $r = 0$, and hence $e|a$. In a similar manner, we can show that $e|d$.

For Claim(ii), all we need to show is that any common divisor f of c and d must divide e. Since $e = ma + nb$, if $f|c$ and $f|d$, proves $f|e$. This completes the proof. ☐

Remark 2.4.2. *The foregoing argument is just an "existence" proof and does not provide a practical method for finding the values of m and n.*

The following theorem illustrates the relation between relatively prime integers and linear combinations(of relatively prime integers).

Theorem 2.4.2. *Let c and d integers, not simultaneously zero. Then c and d are relatively prime if and only if there exist integers m and n such that $1 = mc+nd$.*

Proof. If c and d are relatively prime then $\gcd(c, d) = 1$. By virtue of Theorem 2.4.1, there exist integers m and n satisfying $1 = mc+nd$. In context of converse part, assume that $1 = mc+nd$ for some choice of m and n, and that $e = \gcd(c, d)$. Because $e|c$ and $e|d$, Proposition 2.2.1 yields $e|(mc + nd)$, or $e|1$ implies $e = 1$(Why!), and the desired conclusion follows. ☐

It is true, without adding an extra condition, that $a|c$ and $b|c$ together does not imply $ab|c$. For instance, $6|12$ and $3|12$, but $6 \cdot 3 \nmid 12$. Of course, if $\gcd(6, 3) = 1$, then this situation would not arise. This brings us to Corollary the following corollary:

Corollary 2.4.1. *If $c|e$ and $d|e$, with $\gcd(c, d) = 1$, then $cd|e$.*

Proof. As $c|e$ and $d|e$, there exist integers m and n satisfying $e = mc+nd$. Now the relation $\gcd(c, d) = 1$ implies $1 = ck + dl$ for some choice of integers k and l. Multiplying the last equation by e, we obtain $e = e \cdot 1 = e(ck + dl) = eck + edl$. The appropriate substitutions on the right-hand side allows $e = c(ds)k+d(cr)l = cd(sk + rl)$ implies $cd|e$. ☐

The following few propositions address some properties of greatest common divisors.

Proposition 2.4.2. *Let* a, b *and* c *be integers with* $\gcd(a,b) = d$. *Then*

1. $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.
2. $\gcd(a+cb, b) = \gcd(a,b)$.
3. $\gcd(ma, mb) = md$ $(m > 0)$.

Proof. 1. Here a, b are integers with $\gcd(a,b) = d$. Our claim is $\frac{a}{d}, \frac{b}{d}$ have no common positive divisors other than 1. Assume that e is a positive integer such that $e|\frac{a}{d}$ and $e|\frac{b}{d}$. Then, there are integers k_1 and k_2 with $\frac{a}{d} = k_1 e$ and $\frac{b}{d} = k_2 e$, satisfying $a = dek_1$ and $b = dek_2$. Hence de is a common divisor of a and b. Hence $e = 1$(Why!). Consequently, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2. Here a, b and c be integers with $\gcd(a,b) = d$. Its suffices to show that the common divisors of a, b are exactly the same as the common divisors of $a + cb, b \Rightarrow \gcd(a+cb, b) = \gcd(a,b)$. Let e be a common divisor of a, b. Then $e|(a+cb)$(Why!), such that e is a common divisor of $a+cb, b$. If f is a common divisor of $a+cb, b$ we see that $f|\big((a+cb)-cb\big) = a$(Why!), showing f is a common divisor of a, b. Hence $\gcd(a+cb, b) = \gcd(a,b)$.

3. Since $d = \gcd(a,b)$ then $\exists$ integers x and y such that $d = xa + yb$(by Theorem 2.4.1). Then we have,

$$\begin{aligned} m(xa+yb) &= md \\ \Rightarrow x(ma) + y(mb) &= md \end{aligned}$$

As $m > 0$ then from the above equation we can assert that $\gcd(ma, mb) = m\gcd(a,b) = md$.

□

Proposition 2.4.3. *Prove that* $\gcd(a,c) = 1$ *if and only if* $\gcd(c-a, c)$.

Proof. Every common divisor d of a and c is also a common divisor of $c - a$ and a. Conversely, every common divisor d of $c - a$ and a is also a common divisor of $c - a + a = c$ and a. Therefore the greatest common divisor of a and c is the same as the greatest common divisor of $c - a$ and a. So in general, $\gcd(a,c) = \gcd(c-a, c) = 1$. □

Proposition 2.4.4. *Let* a, b *and* c *be integers with* $\gcd(a,b) = 1$. *Then*

1. *If* $\gcd(a,c) = 1$, *then* $\gcd(a, bc) = 1$.

2. *If* $\gcd(a,b)=1$*, and* $c|a$*, then* $\gcd(b,c)=1$.

3. *If* $c\big|(a+b)$*, then* $\gcd(a,c)=\gcd(b,c)=1$.

4. *If* $d|ac$*, and* $d|bc$*, then* $d|c$.

Proof. 1. Since $\gcd(a,b)=1$, and $\gcd(a,c)=1$, therefore $\exists\ x,y,u,v\in\mathbb{Z}$ such that $1=ax+by=au+cv$.

$$\begin{aligned}\therefore\ 1&=(ax+by)(au+cv),\\&=a(axy+byu+axu)+bcyu,\\&=ak_1+bck_2,\ k_1=axy+byu+axu,\ k_2=yu.\end{aligned}$$

Hence $\gcd(a,bc)=1$.

2. left to the reader.

3. Since $\gcd(a,b)=1,\exists\ u,v\in\mathbb{Z}$ such that $au+bv=1$. Also, $c\big|(a+b)\Rightarrow\exists\ m$ such that $cn=a+b\Rightarrow cn-b=a$.

$$\begin{aligned}\therefore\ (cn-b)u+bv&=1,\\cnu-bu+bv&=1,\\cnu-b(u-v)&=1\Rightarrow\gcd(c,b)=1.\end{aligned}$$

Similarly, $\gcd(c,a)=1$.

4. left to the reader.

☐

Our next theorem seems simple, but is of fundamental importance.

Theorem 2.4.3. *Euclid's Lemma: If* $a|bc$*, with* $\gcd(a,b)=1$*, then* $a|c$.

Proof. By virtue of Theorem 2.4.2, writing $1=am+bn$, where m and n are integers. Multiplication of this equation by c produces $c=1\cdot c=(am+bn)c=acm+bcn$. Because $a|ac$ and $a|bc$, it follows that $a|(acm+bcn)$, which can be recast as $a|c$. ☐

Remark 2.4.3. *The condition* $\gcd(a,b)=1$ *is necessary is evident from the following example:* $12|9\cdot 8$*, but* $12\nmid 9$ *and* $12\nmid 8$.

Theorem 2.4.4. *Let* c,d *be integers, not both zero. For a positive integer* e*,* $e=\gcd(c,d)$ *if and only if*

1. $e|c$ *and* $e|d$.

2. Whenever $f|c$ and $f|d$, then $f|e$.

Proof. Hint: Use Theorem 2.4.1. ☐

Simple application of the last theorem leads to the following proposition.

Proposition 2.4.5. *Let a, b and c be integers with $\gcd(a,b) = 1$, then $\gcd(ac,b) = gcd(c,b)$.*

Proof. Let $\gcd(c,b) = d$. Its suffices to show that $d|ab$ and secondly if $k|ac$ and $k|b$ then $k|d$. Since $d|c$, $\exists\ n$ such that $dn = c$ so $(dn)a = ca \Rightarrow d|ca$.

Next, $\exists\ u, v \in \mathbb{Z}$ such that $d = au + cv$. Since $k|b$, then $\exists\ n$ such that $kn = b$. Hence $d = cu + knv$. Since $\gcd(a,b) = 1\ \exists\ p, q$ such that $ap + bq = 1 \Rightarrow apc + bqc = c$.

$$\begin{aligned} \therefore\ d &= (apc + bqc)x + kny, \\ &= axpc + bqcx + kny. \\ \text{But, } k|ac &\Rightarrow \exists\ r \text{ such that } kr = ac. \\ \therefore\ d &= krpx + knqcx + kny, \\ &= k(rpx + nqcx + ny) \Rightarrow k|d. \end{aligned}$$

Hence using Theorem 2.4.4 we obtain the desired result. ☐

Remark 2.4.4. *The Theorem 2.4.4 sometimes serves as a definition of $\gcd(c,d)$. The advantage of using it as a definition is that order relationship is not involved. Thus, it may be used in algebraic systems having no order relation.*

Euclid's Algorithm

While finding the gcd of two integers (not both 0), we can of course list all the common divisors and pick the greatest one amongst those. However, if a and b are very large integers, the process is very much time consuming. However, there is a far more efficient way of obtaining the gcd. That is known as the Euclid's algorithm. This method essentially follows from the division algorithm for integers.

To prove the Euclidean algorithm, the following lemma will be helpful.

Lemma 2.4.1. *If $a = qb + r$ then the $\gcd(a,b) = \gcd(b,r)$.*

Proof. Let $d = \gcd(a,b)$ and $d_1 = \gcd(b,r)$. Then, $d|a, d|b$ implies $d|(a - qb)$ i.e, $d|r$. Thus d is a common divisor of b and r, hence $d|d_1$. Similarly, $d_1|b, d_1|r$ implies $d_1|(bq + r)$ i.e., d_1 divides both a and b. Then, $d_1|d$. Thus, $d = d_1$, as both d and d_1 are positive by our definition of gcd. ☐

Theorem 2.4.5. *Euclid's Algorithm: Let* a *and* b $(a > b)$ *be any two integers . If* r_1 *is the remainder when* a *is divided by* b*,* r_2 *is the remainder when* b *is divided by* r_1*,* r_3 *is the remainder when* r_1 *is divided by* r_2 *and so on. Thus* $r_{n+1} = 0$*, then the last non zero remainder* r_n *is the* $\gcd(a, b)$*.*

Proof. Euclid's algorithm is an efficient way of computing the gcd of two integers by repeated application of the above lemma. At each step the size of the integers concerned gets reduced. Suppose we want to find the gcd of two integers a and b, neither of them being 0. As $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$, we may assume $a > b > 0$. By performing division algorithm repeatedly, we obtain

$$\begin{aligned}
a &= bq_1 + r_1, & 0 &\le r_1 \le b.\\
b &= r_1q_2 + r_2, & 0 &\le r_2 \le r_1.\\
r_1 &= r_2q_2 + r_3, & 0 &\le r_3 \le r_3.\\
\vdots &= \vdots & &\\
r_{n-2} &= r_{n-1}q_n + r_n, & 0 &\le r_n \le r_{n-1}.\\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, & 0 &\le r_{n+1} \le r_n.
\end{aligned}$$

As we have a decreasing sequence of non-negative integers $b > r_1 > r_2 > \ldots > r_n > r_{n+1}$ we must have $r_{n+1} = 0$ for some n. Then, by applying the previous lemma repeatedly, we find that $\gcd(a, b) = \gcd(r_1, b) = \gcd(r_2, r_1) = \ldots = \gcd(r_{n-1}, r_{n-2}) = \gcd(r_n, r_{n-1}) = r_n$. Thus, the last non-zero remainder r_n in the above process gives us the $\gcd(a, b)$. $\square$

Theorem 2.4.6. *If* $k > 0$*, then* $\gcd(ka, kb) = k\gcd(a, b)$*.*

Let us illustrate the statement of the above theorem with an example: $\gcd(12, 30) = \gcd(3 \cdot 4, 3 \cdot 10) = 3\gcd(4, 10) = 3\gcd(2 \cdot 2, 2 \cdot 5) = 3 \cdot 2\gcd(2, 5) = 6$.

Proof. If each of the equations appearing in the Euclidean Algorithm for a and b is multiplied by k, we obtain

$$\begin{aligned}
ak &= (bk)q_1 + r_1k, & 0 &\le r_1k \le bk.\\
bk &= (r_1k)q_2 + r_2k, & 0 &\le r_2k \le r_1k.\\
r_1k &= (r_2k)q_2 + r_3k, & 0 &\le r_3k \le r_3k.\\
\vdots &= \vdots & &\\
r_{n-2}k &= (r_{n-1}k)q_n + r_nk, & 0 &\le r_nk \le r_{n-1}k.\\
r_{n-1}k &= (r_nk)q_{n+1} + 0. & &
\end{aligned}$$

But here the Euclidean Algorithm applied to the integers ak and bk, so that their greatest common divisor is the last nonzero remainder $r_n k$; that is, $\gcd(ka, kb) = r_n k = k \gcd(a, b)$. □

Based on the above theorem, let us state and prove the following corollary:

Corollary 2.4.2. *Its suffices to consider the case $k < 0$. Then $-k = |k| > 0$ and*

$$\begin{aligned}\gcd(ka, kb) &= \gcd(-ka, -kb)\\ &= \gcd(|k|a, |k|b)\\ &= |k| \gcd(a, b).\end{aligned}$$

2.5 Least Common Multiple

There is a concept parallel to that of the greatest common divisor of two integers, known as their least common multiple. Prime factorizations can also be used to find the smallest integer that is a multiple of two positive integers(treated in later chapters). The problem of finding this integer arises when fractions are added.

Definition 2.5.1. *The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by a and b, denoted by $lcm(a, b)$ or $[a, b]$.*

The above definition can also be formulated as follows:

Definition 2.5.2. *The least common multiple of two nonzero integers a and b is the positive integer l satisfying the following:*

1. *$a|l$ and $b|l$.*
2. *If $a|c$ and $b|c$, with $c > 0$, then $l \leq c$.*

Example 2.5.1. *We have the following least common multiple: $lcm(16, 20) = 80, lcm(24, 36) = 72, lcm(4, 20) = 20$, and $lcm(5, 13) = 65$.*

Remark 2.5.1. *Given nonzero integers a and b, $lcm(a, b)$ always exists and $lcm(a, b) < |ab|$(Verify!).*

Proposition 2.5.1. *For nonzero integers a and b, the following statements are equivalent(TFAE):*

1. $\gcd(a, b) = |a|$.

2. $a\big|b$.

3. $lcm(a,b) = |b|$.

Proof. (1)$\Rightarrow$(2): Let (1) holds. Then $\exists\ n \in \mathbb{Z}$ such that $b = \big|a\big|n$. Now $a > 0 \Rightarrow b = an \Rightarrow a|b$. Again, $a < 0 \Rightarrow |a| = -1 \Rightarrow b = (-a)n \Rightarrow b = a(-n) \Rightarrow a|b$. $a|b$. Hence (2) holds.

(2)$\Rightarrow$(3): Let (2) holds. Then $a\big||b|$ and clearly $b\big||b|$. Let c be another common multiple. Then $a\big|c$ and $b\big|c$ with $c > 0$. Now $b\big|c$ implies $\exists\ n \in \mathbb{Z}$ such that $c = bn$ and $\big|n\big| \geq 1$. Thus, $|c| = |b||n| \geq b$ which further gives $|c| \geq |b|$ and by definition $|b| = lcm(a,b)$.

(3)$\Rightarrow$(1): Let (3) holds. Therefore $a\big||b| \Rightarrow |a|\big||b|$. Let c be another common multiple. Then $\exists\ n \in \mathbb{Z}$ such that $a = cn \Rightarrow |a| = |c||n|$. But $|n| \geq 1 \Rightarrow |c||n| \geq |c| \Rightarrow |a| \geq |c|$.Therefore $\gcd(a,b) = |a|$. □

The following theorem filled the gap between greatest common divisor and least common multiple.

Theorem 2.5.1. *If a and b are positive integers, then $[a,b] = \dfrac{ab}{(a,b)}$, where $[a,b]$ and (a,b) are the least common multiple and greatest common divisor of a and b, respectively.*

Proof. Let us begin with taking $c = (a,b)$ and write $a = cr, b = cs$ for integers r and s. If $l = \dfrac{ab}{c}$, then $l = as = rb$, making l a (positive) common multiple of a and b.

Now let d be any positive integer that is a common multiple of a and b, implies $d = au = bv$. As we know, there exist integers k and l such that $c = ak + bl$. As a result of which,

$$\frac{d}{l} = \frac{dc}{ab} = \frac{d(ak+bl)}{ab} = \frac{d}{b}k + \frac{d}{a}l = vk + ul \Rightarrow l|c \Rightarrow l \leq c.$$

Hence $l = lcm(a,b)$ and $[a,b] = \dfrac{ab}{(a,b)}$. □

Remark 2.5.2. *The alternate proof of the above theorem can be done using the prime factorizations of integers a and b (for further details refer to chapter Prime Numbers).*

Corollary 2.5.1. *For any choice of positive integers a and b, $[a,b] = ab$ if and only if $(a,b) = 1$.*

Proof. Obvious. □

We conclude this section with a simple but interesting proposition.

Proposition 2.5.2. *For a and b be two non zero integers. Then*

1. $\gcd(a,b) = lcm(a,b)$ *if and only if* $a = \pm b$.
2. *If* $k > 0$, *then* $lcm(ka,kb) = k\ lcm(a,b)$.
3. *If* m *is any common multiple of* a *and* b, *then* $lcm(a,b)\big|m$.

Proof. 1. Let us consider $\gcd(a,b) = lcm(a,b) = d$. Now by Theorem 2.5.1 we get $d = ab$. Since $d\big|a$ then $\exists x \in \mathbb{Z}$ such that $dx = a$. This implies $d^2 = dxb \Rightarrow d = xb \Rightarrow b\big|d$. Thus we have $d\big|b$ and $d\big|b$ which together implies $d = \pm b$(by Proposition 2.2.1). By similar arguments we also have $d = \pm a$. Therefore $|d| = |a| = |b|$ implying $a = \pm b$.

Conversely let $d = \pm a$ holds. Then again by Proposition 2.2.1 we can assert that $a\big|b$ and $b\big|a$. This claims that $\gcd(a,b) = lcm(a,b)$.

2. To prove this we are to start with $\gcd(ka,kb)\cdot lcm(ka,kb) = k^2|ab|$. Then,

$$\begin{aligned} k\gcd(a,b)\cdot lcm(ka,kb) &= k^2|ab| \text{ [by Proposition 2.4.2]} \\ \Rightarrow \gcd(a,b)\cdot lcm(ka,kb) &= k|ab| \\ \Rightarrow \gcd(a,b)\cdot lcm(ka,kb) &= k\gcd(a,b)\cdot lcm(a,b) \\ \Rightarrow lcm(ka,kb) &= k\ lcm(a,b). \end{aligned}$$

3. Let us consider $l = lcm(a,b)$ and by division algorithm $\exists$ integers q and r such that $m = lq + r,\ 0 \le r < l$.

If $r = 0$ then obviously $l\big|m$.

If $0 < r < l$ then we can write $r = m - lq$. Since m and l are multiples of a and b then $\exists$ integers x,y,u,v such that $r = ax - ayq = a(x - yq)$ and also $r = bu - bvq = b(u - vq)$. This shows that r is a multiple of a, b and this contradicts the fact $l = lcm(a,b)$. So $r < l$ is not possible. This proves our assertion.

□

2.6 Worked out Exercises

Problem 2.6.1. *If* a,b,c *are integers, then* $\gcd(a,bc) = 1$ *if and only if* $\gcd(a,b) = \gcd(a,c) = 1$.

Solution 2.6.1. *Let* $\gcd(a,b) = \gcd(a,c) = 1$ *holds. Then there exists integers* m_1, n_1, m_2 *and* n_2 *satisfying*

$$am_1 + bn_1 = 1 = am_2 + cn_2.$$

Therefore

$$am_1cn_2 + bn_1cn_2 = cn_2 = 1 - am_2,$$
$$\Rightarrow a(m_2 + cm_1n_2) + bc(n_1n_2) = 1.$$

As $m_2 + cm_1n_2$ *and* n_1n_2 *are integers, therefore* $\gcd(a,bc) = 1$.

Conversely, let $\gcd(a,bc) = 1$ *holds. We are to show* $\gcd(a,b) = \gcd(a,c) = 1$. *Let* $\gcd(a,b) \neq 1$. *Then* $\gcd(a,b) = d$ *implies there exists* m, n *such that*

$$am + bn = d$$
$$\Rightarrow acm + bcn = cd$$
$$\Rightarrow a(cm) + b(cn) = cd.$$

Therefore $\gcd(a,bc) = cd (\neq 1)$, *a contradiction. Thus both* a, b *and* a, c *are coprime.*

Problem 2.6.2. *Prove or disprove: If* $a|(b+c)$, *then either* $a|b$ *or* $a|c$.

Solution 2.6.2. *Hint: Take* $a = 3, b = 2, c = 7$.

Problem 2.6.3. *If* $a|bc$, *show that* $a|\gcd(a,b)\gcd(a,c)$.

Solution 2.6.3. *Let* $\gcd(a,b) = d_1$ *and* $\gcd(a,c) = d_2$. *Then* $\exists\, x, y, u, v \in \mathbb{Z}$ *such that*

$$d_1 = ax + by, \ \& \ d_2 = au + cv.$$

Also, $\exists\, n \in \mathbb{Z}$ *satisfying* $an = bc$. *Now,*

$$\begin{aligned} d_1d_2 &= (ax+by)(au+cv), \\ &= a^2xu + acxv + abuy + bcyv, \\ &= a(axu + cxv + buy) + anyv, \\ &= a(axu + cxv + buy + nyv). \end{aligned}$$

$$\therefore\ a|\gcd(a,b)\gcd(a,c).$$

Problem 2.6.4. *Prove that if* $d|n$, *then* $(2^d - 1)|(2^n - 1)$.

Solution 2.6.4. *We know that*

$$\begin{aligned} a^n - 1 &= (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1), \\ \therefore\ 2^n - 1 &= (2-1)(2^{n-1} + 2^{n-2} + \ldots + 2 + 1), \\ \therefore\ 2^d - 1 &= (2-1)(2^{d-1} + 2^{d-2} + \ldots + 2 + 1). \end{aligned}$$

Since $d|n$, $\exists\, x \in \mathbb{Z}$ *such that* $dx = n$. *Therefore*

$$\begin{aligned} 2^n - 1 = 2^{dx} - 1 &= (2^d)^x - 1, \\ &= (2^d - 1)(2^{d(x-1)} + 2^{d(x-2)} + \ldots + 2^d + 1). \end{aligned}$$

$$\therefore\ (2^d - 1)\big|(2^n - 1).$$

Problem 2.6.5. *Prove that the product of any three consecutive integers is divisible by* 6.

Solution 2.6.5. *Here we need to show* $6|a(a+1)(a+2)$, *for any arbitrary* $a \in \mathbb{Z}$.

Let $S = a(a+1)(a+2)$. *Here* $6 = 3 \cdot 2$ *and* $\gcd(2,3) = 1$. *If* a *is even, then* $2|a \Rightarrow 2|S$. *And if odd, then* $2\big|(a+1) \Rightarrow 2|S$. *Let* $a = 3q + r$, $q, r \in \mathbb{Z}$. *Now* $r = 0, 1, 2$. *For all the values of* r, $3|S$ *(verify!). Hence* $2|S, 3|S$ *together implies* $6|S$.

Problem 2.6.6. *If* a *is an odd integer, then* $24|a(a^2-1)$.

Solution 2.6.6. *Let us first prove,* a *is of the form* $8k+1$. *Let* $a = 4q + r$. *Therefore* $r = 0$ *or* 3 *(Why!). Therefore*

$$\begin{aligned} a^2 &= 16q^2 + 8q + 1 = 8k + 1, \text{ for } r = 0 \\ a^2 &= 16q^2 + 24q + 9 = 8k' + 1, \text{ for } r = 3. \end{aligned}$$

So $a(a^2-1) = a(8k)$, *for some* k. *Hence* $8\big|a(a^2-1)$. *Therefore* $6\big|a(a^2-1) \Rightarrow 3|a(a^2-1)$. *As* $\gcd(3,8) = 1$, *hence* $24|a(a^2-1)$ *(Why!).*

Problem 2.6.7. *If* a *is an integer not divisible by* 2 *or* 3, *then* $24|(a^2+23)$.

Solution 2.6.7. *Let* $a = 12q + r$, $q, r \in \mathbb{Z}$ *with* $0 \le r < 12$. *But here,* $r = 1, 5, 7, 11$ *(Why!). Now*

$$\begin{aligned} a^2 + 23 &= (12q + r)^2 + 23, \\ &= 144q^2 + 24qr + r^2 + 23, \\ &= 24(6q^2 + qr) + r^2 + 23. \end{aligned}$$

$$\begin{aligned}
\textit{Now, } r = 1 &\textit{ gives } r^2 + 23 = 24\\
r = 5 &\textit{ gives } r^2 + 23 = 48 = 24 \cdot 2\\
r = 7 &\textit{ gives } r^2 + 23 = 72 = 24 \cdot 3\\
r = 11 &\textit{ gives } r^2 + 23 = 144 = 24 \cdot 6\\
\therefore\ a^2 + 23 &= 24(6q^2 + qr) + 24 \cdot k, \textit{ for some } k.
\end{aligned}$$

Hence $24|(a^2 + 23)$.

Problem 2.6.8. *For* $n \geq 1$, *and positive integers* a, b, *prove that* $\gcd(a^n, b^n) = 1$ *where* $\gcd(a, b) = 1$.

Solution 2.6.8. *For* $n = 1$, *the statement is obvious. Let us assume the statement be true for* $n(> 1) = k$ *i.e.* $\gcd(a^k, b^k) = 1$. *Now* $\gcd(a^k, b^{k+1}) = \gcd(a^k, b^k) = 1$*[refer to the properties of GCD]. Since* $\gcd(a, b) = \gcd(b, a) = 1$, *then* $\gcd(a^k, b^{k+1}) = 1 = \gcd(a^{k+1}, b^{k+1})$.

Problem 2.6.9. *For* $n \geq 1$, *and positive integers* a, b, *prove that the relation* $a^n|b^n$ *implies* $a|b$.

Solution 2.6.9. *The relation is obvious for* $n = 1$. *If possible, let us assume the relation is true for* $n = k$. *Then* $a^n|b^n$ *implies* $a|b$, *which further implies* $\exists\ x, y$ *such that*

$$b^k = xa^k \ \&\ b = ay.$$

$$\therefore\ xa^{k+1} = ab^k = \left(\frac{b}{y}\right) b^k = \frac{b^{k+1}}{y}.$$

$$\therefore\ xya^{k+1} = b^{k+1} \Rightarrow a^{k+1}|b^{k+1}.$$

Problem 2.6.10. *Prove that if* $\gcd(a, b) = 1$, *then* $\gcd(a + b, ab) = 1$.

Solution 2.6.10. *Let* c *be the common divisor of* $a+b$ *and* ab. *Then* $\gcd(a, c) = \gcd(b, c) = 1$. *Since* $c\big|ab$ *and* $\gcd(c, a) = 1$, *then by Euclid's Lemma we have* $c\big|b$. *By similar reasoning,* $c\big|a$. *As* $c \leq \gcd(a, b) = 1 \Rightarrow c = 1 \Rightarrow \gcd(a + b, ab) = 1$.

Problem 2.6.11. *Prove that the greatest common divisor of two positive integers divides their least common multiple.*

Solution 2.6.11. *Let* $a, b > 0$. *We are to prove* $\gcd(a, b)\big|lcm(a, b)$. *We know that* $\gcd(a, b)lcm(a, b) = ab$. *Let* $d = \gcd(a, b)$. *Then* $\exists$, m, n *such that* $a = dn, b = dm$.

$$\begin{aligned}
&d \cdot lcm(a, b) = (dn)(dm).\\
&\therefore\ lcm(a, b) = d(nm) \Rightarrow d\big|lcm(a, b) \Rightarrow \gcd(a, b)\big|lcm(a, b).
\end{aligned}$$

Problem 2.6.12. *If a and b are prime to each other then prove that* $\gcd(a+b, a^2+b^2) = 1$ *or* 2.

Solution 2.6.12. *Let* $\gcd(a+b, a^2+b^2) = d$. *Then* $d\big|(a^2+b^2) \iff d\big|(a+b)(a-b)+2b^2$. *Since* $d\big|(a+b)$, $\exists\ x$ *such that* $dx = a+b$. *Let* $m \in \mathbb{Z}$ *be such that*

$$dm = (a+b)(a-b)+2b^2 \Rightarrow dm = dx(a-b)+2b^2 \Rightarrow d[m-x(a-b)] = 2b^2 \Rightarrow d\big|2b^2.$$

Now combining the facts $d\big|(a+b)$ *and* $\gcd(a,b) = 1$, *we find* $\gcd(b,d) = 1$*(Why!). Thus we get* $d \nmid b$, *which implies* $d|2$. *Therefore* $d \leq 2$ *implies* $d = 1$ *or* 2.

Problem 2.6.13. *Let a, b, c be integers, no two of which are zero, and* $d = \gcd(a,b,c)$. *Show that* $d = \gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b)$.

Solution 2.6.13. *Firstly, we will show* $d = \gcd(\gcd(a,b),c)$. *Let* $f = \gcd(a,b)$ *and* $g = \gcd(f,c)$. *Now* $g|f \Rightarrow g|a, g|b$. *Here* $g|c \Rightarrow g \leq d$. *Our next task is to show* $d|f$. *Here for some* $x, y \in \mathbb{Z}$, $f = ax+by$*[refer to Theorem 2.4.1]. Now* $a = du, b = dv$ *for some* $u, v \in \mathbb{Z}$. *Hence* $f = dux+dvy \Rightarrow d|f$. *Now* $d|c \Rightarrow d|g \Rightarrow d \leq g$. *Hence combining,* $d = g$ *holds i.e.* $d = \gcd(\gcd(a,b),c)$. *Proceeding as above, we can show that* $d = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b)$. *Thus* $d = \gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c)) = \gcd(\gcd(a,c),b)$.

2.7 Linear Diophantine Equations

Before delving deep into the topic, let us start with the following problem:

A person wishes to buy ice cream bar for a get-together at home. After going to the ice cream parlour he came across with some flavours: one is chocolate bar costing Rs.126 and another is strawberry bar costing Rs.99. He decided to buy both combinations with a budget of Rs.2000. Now the problem is; whether there exist any such combinations of these two flavours? To answer this, let k denote the number of chocolate bars and l denote the number of strawberry bars, the person can purchase. Then we must have $126k + 99l = 2000$, where both k and l are nonnegative integers.

Now the need for Diophantine equation get along to find the solutions of a particular equation, which follow from the set of integers. Diophantine equations get their name from the ancient Greek mathematician Diophantus, who wrote extensively on such equations. The type of diophantine equation $ak + bl = c$, where a, b and c are integers is called a linear diophantine equations in two variables. We now develop the theory for solving such equations. The following theorem illustrates that when such an equation has solutions, and when there are solutions, explicitly describes them.

Theorem 2.7.1. *Let* a, b *be positive integers with* $d = \gcd(a, b)$*. If* $d \nmid c$*, the equation* $ax + by = c$ *has no solutions(in integers). There are infinitely many solutions(integers) if* $d|c$*. Moveover in particular, if* $x = x_0, y = y_0$ *is a solution of the equation, then all solutions are given by*

$$x = x_0 + \frac{b}{d}n, \;\; y = y_0 - \frac{a}{d}n, \; n \textit{ being an integer.}$$

Before proceeding for the proof, first we demonstrate the above theorem for finding all the integral solutions of the two diophantine equations described at the beginning of this section. We first consider the equation $126x + 99y = 2000$. The greatest common divisor of 126 and 99 is $\gcd(99, 126) = 9$. Since $9 \nmid 2000$, we can say no integral solutions exist. Hence no combination of 126 and 99 rupees he can purchase.

Proof. Assume that x and y are integers satisfying $ax + by = c$. Together $d|a$ and $d|b$ implies $d|c$(Why!). Hence if $d \nmid c$ there does not exists any integral solutions. So we assume that $d|c$. Then from theorem (2.4.1), for some integers s, t

$$d = as + bt. \tag{2.7.1}$$

Since, $d|c$ there exist some integer e such that $de = c$ holds. Multiplying (2.7.1), we obtain

$$c = a(se) + b(te).$$

Hence one particular solution of the equation is given by $x = x_0 = se, y = y_0 = te$.

Now, to prove the remaining part of the theorem suppose $x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n$, n being an integer. Since,

$$ax + bl = a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) = ax_0 + bl_0 = c,$$

we see that (x, y) is a solution.

Next our claim is to show every solution of the equation $ax + bl = c$ must be of the form described in the theorem. since,

$$ax_0 + bl_0 = c,$$

on subtraction we obtain

$$a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = b(-y + y_0). \tag{2.7.2}$$

Dividing both sides by d, we see that

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(-y + y_0).$$

By virtue of Proposition 2.4.2, we know $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Also, using Euclid's Lemma it follows $\frac{a}{d}|(y_0 - y)$. Hence there exists an integer n with $\frac{a}{d}n = y_0 - y$ means $y = y_0 - \frac{a}{d}n$. Now putting this value of y into the (2.7.2), we find $a(x - x_0) = b\left(\frac{a}{d}\right)n$ implies $x = x_0 + \left(\frac{b}{d}\right)n$. □

Example 2.7.1. *A man wishes to purchase Rs* 510 *of travelers checks. The checks are available only in denominations of Rs* 20 *and Rs* 50*. How many of each denomination should he buy?*

Answer 2.7.1. *Consider the equation* $20k + 50l = 510$*. The greatest common divisor of* 20 *and* 50 *is* $(20, 50) = 10$*, and since* $10|510$*, there are infinitely many integral solutions. Using the Euclidean algorithm, we find that* $20(-2) + 50 = 10$*. Multiplying both sides by* 51*, we obtain* $20(-102) + 50(51) = 510$*. Hence a particular solution is given by* $k_0 = -102$ *and* $l_0 = 51$*. Theorem 2.7.1 tells us that all integral solutions are of the form* $k = -102 + 5n$ *and* $l = 51 - 2n$*. Since we want both* k *and* l *to be nonnegative, we must have* $-102 + 5n > 0$ *and* $51 - 2n > 0$*; thus,* $n > \frac{102}{5}$ *and* $n < \frac{51}{2}$*. Since* n *is an integer, it follows that* $n = 21, 22, 23, 24, 25$*. Hence we have the following* 5 *solutions:* $(k, l) = (3, 9), (8, 7), (13, 5), (18, 3), (23, 1)$*.*

2.8 Worked out Exercises

Problem 2.8.1. *Examine the nature of the following Diophantine equations:*

1. $14x + 35y = 93$.
2. $33x + 14y = 115$.

Solution 2.8.1. *1. Here* $\gcd(14, 35) = 7$ *and* $7 \nmid 93$*, hence not solvable.*

2. Here $\gcd(33, 14) = 1$ *and* $1\big|115$*, hence solvable.*

Problem 2.8.2. *Determine all solutions, in positive integers, of the following Diophantine equations:*

1. $158x - 57y = 7$.

2. $54x + 21y = 906$.

Solution 2.8.2. *1. To find the solution of this equation we need to find the* gcd *of* $158, 57$*. Now applying Euclid's Algorithm, we obtain*

$$\begin{aligned} 158 &= 3\cdot 57 - 13 & \textit{Again } 1 &= 3 - 2 = 3 - (5-3)\\ 57 &= 4\cdot 13 + 5 & &= 2\cdot 3 - 5 = 2(13 - 2\cdot 5) - 5\\ 13 &= 2\cdot 5 + 3 & &= 2\cdot 13 - 5\cdot 5\\ 5 &= 3\cdot 1 + 2 & &= 2\cdot 13 - 5(57 - 4\cdot 13)\\ 3 &= 2\cdot 1 + 1 & &= 22\cdot 13 - 5\cdot 57\\ & & &= 22(3\cdot 57 - 158) - 5\cdot 57\\ & & &= 61(57) + (-22)\cdot 158.\\ \textit{Thus, } \gcd(158,57) &= 1. & \therefore 7 &= (61\cdot 7)57 + (-22\cdot 7)158. \end{aligned}$$

Since $\gcd(158, 57)|7 = 7$ *therefore, an integral solution do exist for the given equation. Hence* $(x_0, y_0) = (-154, -427)$ *is an integral solution. Hence all integral solutions of the given equation is of the form,*

$$\begin{aligned} x &= -154 + \frac{-57}{1}n = -154 - 57n > 0 & &\Rightarrow n < -2.7 \Rightarrow n \le -3\\ y &= -1510 + \frac{-158}{1}n = -1510 - 158n > 0 & &\Rightarrow n < -2.7 \Rightarrow n \le -3. \end{aligned}$$

2. To find the solution of this equation we need to find the gcd *of* $54, 21$*. Now applying Euclid's Algorithm, we obtain,*

$$\begin{aligned} 54 &= 2\cdot 21 + 12 & \textit{Again, } 3 &= 12 - 9 = 12 - (21 - 12)\\ 21 &= 12\cdot 1 + 9 & &= 2\cdot 12 - 21\\ 12 &= 9\cdot 1 + 3 & &= 2(54 - 2\cdot 21) - 21\\ 9 &= 3\cdot 3 + 0 & &= 2\cdot 54 + (-5)\cdot 21.\\ \textit{Thus, } \gcd(54,21) &= 3 \;\&\; 3\big|906. & \therefore 906 &= (302\cdot 2)54 + (302\cdot(-5))21. \end{aligned}$$

Since $\gcd(54, 21)|906 = 302$ *therefore, an integral solution do exist for the given equation. Hence* $(x_0, y_0) = (604, -1510)$ *is an integral solution. Hence all integral solutions of the given equation is of the form,*

$$\begin{aligned} x &= 604 + \frac{21}{3}n = 604 + 7n > 0 & &\Rightarrow n > -86.3\\ y &= -1510 + \frac{-54}{3}n = -1510 - 18n > 0 & &\Rightarrow n < -83.9. \end{aligned}$$

Thus, $n = -84, -85, -86,$ *which gives* $(x, y) = (16, 2), (9, 20), (2, 38)$.

Problem 2.8.3. *Determine all solutions of the Diophantine equation* $24x + 138y = 18$.

Solution 2.8.3. *First we need to calculate the gcd of* 24 *and* 138 . *Here,*

$$\begin{aligned} 138 &= 5\cdot 24+18 & \textit{Again, } 6 &= 24-18 \\ 24 &= 18+9 & &= 24-(138-5\cdot 24)\\ 18 &= 3\cdot 6+0 & &= 6\cdot 24-138\\ \textit{Thus, } \gcd(24,138) &= 6 \ \&\ 6\big|18. & \therefore 18 &= (18)54+(-3)138. \end{aligned}$$

So the integral solution is $x_0 = 18,\ y_0 = -3$. *Thus the solution of this equation is,*

$$\begin{aligned} x &= 18 + \left(\frac{138}{6}\right)n = 18 + 23n \\ y &= -3 - \left(\frac{24}{6}\right)n = -3 - 4n \ [n \in \mathbb{Z}]. \end{aligned}$$

Problem 2.8.4. *A farmer purchased* 100 *heads of livestock for a total cost of Rs.*4000. *Prices were as follow: sheep, Rs.*120 *each; hen, Rs.*25 *each; duck, Rs.*50 *each. If the farmer obtained at least one animal of each type how many had he bought?*

Solution 2.8.4. *Let us consider the variables* x, y *and* z *for sheep, hen and duck respectively. Then from given hypothesis we have,* $x + y + z = 100$ *and* $120x + 25y + 50z = 4000$, *where* $x, y, z \geq 1$. *Then* $24x + 5y + 10z = 800$ *and* $24x + 10z + 5(100 - x - z) = 800$ *holds. Combining last two equations yield* $19x + 5z = 300$. *Hence the solutions are* $x = 0,\ z = 60$. *Therefore*

$$\begin{aligned} x &= 5k,\ z = 60 - 19k, \\ y &= 40 + 14k,\ k \in \mathbb{Z}. \end{aligned}$$

Consequently,

$$\begin{aligned} 5k \geq 1 &\Rightarrow k \geq 1 \\ 60 - 19k \geq 1 &\Rightarrow k \leq 3 \\ 40 + 14k \geq 1 &\Rightarrow k \geq -2. \end{aligned}$$

Considering last three inequalities, we get $1 \leq k \leq 3 \Rightarrow k = 1, 2, 3$. *Therefore the possibilities are* 5 *sheep,* 54 *hens and* 41 *ducks or* 10 *sheep,* 68 *hens and* 22 *ducks or* 15 *sheep,* 82 *hens and* 3 *ducks.*

2.9 Exercises:

1. Let a, b and c be integers with $\gcd(a, b) = 1$. Then $\gcd(a^2, b^2) = 1$.
2. Verify that $3a^2 - 1$ is never a perfect square.
3. For $n \geq 1$, establish that the integer $n(7n^2 + 5)$ is of the form $6k$.
4. For an odd integer n, show that $n^4 + 4n^2 + 11$ is of the form $16k$.
5. Verify that if an integer is simultaneously a square and a cube (as is the case with $64 = 8^2 = 4^3$), then it must be either of the form $7k$ or $7k + 1$.
6. If $a \big| bc$, show that $a \big| \gcd(a, b)\gcd(a, c)$.
7. Verify the followings:
   (a)the product of any four consecutive integers is divisible by 24;
   (b)the product of any five consecutive integers is divisible by 120.
8. Prove that the expression $\frac{(3n)!}{(3!)^n}$ is an integer for all $n \geq 0$.
9. Establish each of the statements below:
   (a)If a and b are odd integers, then $8 \big| (a^2 - b^2)$.
   (b)If a is an arbitrary integer, then $6 \big| a(a^2 + 11)$.
10. Assuming that $\gcd(a, b) = 1$, prove that $\gcd(2a + b, a + 2b) = 1$ or 3.
11. Prove that if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.
12. Find integers x, y, z satisfying $\gcd(198, 288, 512) = 198x + 288y + 512z$.
13. Use the Euclidean Algorithm to obtain integers x and y satisfying $\gcd(1769, 2378) = 1769x + 2378y$.
14. Examine the nature of the Diophantine equation $14x + 35y = 93$.
15. Determine all solutions in the positive integers of $158x - 57y = 7$.
16. Determine all solutions in the integers of $221x + 35y = 11$.
17. Mr.Sen had gone to a medical shop to buy two medicines: medicine A and medicine B. By mistake, the chemist had given him the number of medicine A in place of medicine B and vice versa.Unaware of the fact, Mr.Sen received an extra amount Rs.68 from the shop keeper. Considering the price of each medicine A and medicine B to be Rs.10 and Rs.15 respectively, find the least number of medicine A, Mr. Sen wanted to purchase.

18. One hundred packets of dry food are distributed among 100 persons in such a way that every man, woman and child receives 3 packets, 2 packets, and half a packet respectively. Find the total number of persons over there?

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

3

Prime Numbers

> *“God may not play dice with the universe, but something strange is going on with the prime numbers.”*
>
> – Paul Erados,

3.1 Introduction

A prime number is an integer or a whole number that has only two factors 1 and itself. In other words, a prime number can be divided only by 1 and itself. Also primes are greater than 1. For example, 3 is prime as it fails to be divided evenly by any number except for 1 and 3. However, 6 is not because it can be evenly divided by 2 and 3.

The largest known prime number is $2^{82,589,933} - 1$, a number which has $24,862,048$ digits when written in base 10. It was discovered by Patrick Laroche of the great internet Mersenne Prime search. Euclid recorded a proof that there does not exist any largest prime number and many mathematicians continue to search for large prime numbers.

In 1978, few researchers used prime numbers to scramble and unscramble coded messages. This early form of encryption smoothen the way for Internet security, putting prime numbers at the heart of electronic commerce. Public-key cryptography, or RSA encryption, has simplified secure transactions of all times. The security of this type of cryptography depends on the difficulty of factoring large composite numbers, which is the product of two large prime numbers. Also, in modern banking security systems depend on the fact that large composite numbers cannot be factored in a short amount of time. Two primes are considered secure if they are $2,048$ bits long, because the product of these two primes would be about $1,234$ decimal digits.

Prime numbers have shown its existence in nature. Cicadas insect spend most of their time hiding, only reappearing to mate every 13 or 17 years. Why this particular number? Scientists invented that cicadas reproduce in cycles that minimize possible interactions with predators. Any predator reproductive cycle that divides the cicada's cycle evenly means that the predator will hatch out the same time as the cicada at some point. For instance , if the cicada evolved towards a 12-year reproductive cycle, predators who reproduce at the 2, 3, 4 and 6 year intervals would find themselves with plenty of cicadas to eat. By using a reproductive cycle with a prime number of years, cicadas would be able to minimize contact with predators. Simulation models of $1,000$ years of cicada evolution prove that there is a major advantage for reproductive cycle times based on primes.

3.2 Primes & Fundamental Theorem of Arithmetic

Positive divisors of an integer have a great importance in the study of number theory. The integer 1 has only one positive divisor which is 1 itself. Any other integers has more than one divisor. At Least two divisors of them are 1 and the integer itself. There are integers which have divisors other than 1 and itself. The numbers which have only two divisors 1 and itself are called prime numbers.

Definition 3.2.1. *An integer $p > 1$ is said to be a prime number or prime if its only divisors are 1 and p itself.*

An integer which is not prime is known to be a composite number, having more than two(what are those?) divisors.

Among the first ten positive integers $2, 3, 5, 7$ are prime numbers whereas $4, 6, 8, 9, 10$ are examples of composite numbers. Here 1 is a special type of integer which is neither prime nor composite. Here the study of prime numbers starts with the study of prime divisors. Here 5 is prime where $5 \nmid 3$ but $5|5$ itself together implies $5|15$, leads us to the following theorem:

Theorem 3.2.1. *An integer $p > 1$ is prime if and only if $p|ab$ implies $p|a$ or $p|b$.*

Proof. Let p be a prime number such that for any two integers a and b, $p|ab$ holds. If $p|a$, then we are done. Let $p \nmid a$ then the only divisors of p are 1 and p

itself. As p is prime we have $\gcd(p, a) = 1$ implies there exists integers r, t such that $1 = rp + at$. Then $b = brp + t(ab)$. Now $p|ab$ and $p|prb$ imply $p|b$.

Conversely, let p satisfy the condition and q, r be any integers such that $p = qr$ where $q < p$. Thus $p|qr$ and by the condition we can say either $p|q$ or $p|r$. But $q|p$ shows $p|r$ only. Therefore $r = pt$ for some integer t. Hence $p = qr = qpt$ implies $qt = 1$ implies $q = 1$. So 1 and p are only divisors of p. This shows p is prime. ☐

Let us now generalize the above theorem for more than two terms as follows:

Theorem 3.2.2. *If p is prime and $p|a_1 a_2 a_3 \cdots a_n$, then $p|a_i$ for some $i = 1, 2, 3, \ldots, n$.*

Proof. We will prove this by mathematical induction. The statement is true for $n = 1$. With reference to theorem (3.2.1) the statement is true for $n = 2$. Let us assume the statement is true for $n = k$. Let $n = k + 1$ holds. Then $p|a_1 a_2 a_3 \cdots a_k a_{k+1}$. Also choose $a_1 a_2 a_3 \cdots a_k = b$ where b is an integer, thus $p|ba_{k+1}$. Now if $p|a_{k+1}$ we are done. If $p \nmid a_{k+1}$, then from $n = 2$ we have $p|b$ implies $p|a_1 a_2 a_3 \cdots a_k$ which further implies $p|a_i$ for some i by the induction hypothesis. Thus $p|a_i$ for $i = 1, 2, \ldots, k+1$. So the statement is true for $n = k+1$. Thus by principle of mathematical induction the theorem is proved. ☐

Corollary 3.2.1. *If $p, q_1, q_2, q_3, \ldots, q_n$ are all primes and $p|q_1 q_2 q_3 \cdots q_n$ then $p = q_i$ for some $i = 1, 2, \ldots, n$.*

Proof. By virtue of above theorem, we know that if $p|q_i$ for some $i = 1, 2, \ldots, n$. But q_i being prime so q_i is not divisible by any integer other than 1 and itself. Since, $p > 1$ then we have $p = q_i$ for some $i = 1, 2, 3 \ldots, n$. ☐

Let us now consider few integers $35, 25, 10$ and we see that $7|35, 5|25$ and $2|10$. So the observation is that every integer has a prime factor. We now prove this result for any integer $n \geq 2$.

Theorem 3.2.3. *Every integer $n \geq 2$ has a prime factor.*

Proof. We prove the statement by mathematical induction method. Taking $n = 2$, the result is obvious as 2 itself is prime. Let us assume that each of the integers $2, 3, \ldots, n - 1$ has a prime factor. Now considering $n > 2$ we can say that the result is true if n is prime. If n is composite then $n = rs$ for some integer r, s with $1 < r, s < n$. Then by induction hypothesis r has a prime factor which is also a prime factor of n. So the theorem is proved. ☐

The set of all positive integers is countably infinite and the set of prime numbers is a subset of the set. So two possibilities to occur. One, the cardinality of the set is finite and the other which is countably infinite. But the set of prime numbers that are countably infinite is given in a theorem of Euclid (300 B.C.) and till the 21st century the proof is considered as an elegant proof of Mathematics.

Theorem 3.2.4. *Prime number set is countably infinite.*

Proof. Let the number of primes be finite and we write them as $p_1 = 2, p_2 = 3 \cdots p_n$. Now let us consider a composite number $m = p_1 p_2 \cdots p_n + 1$ and $m > 1$. As m is composite it has a prime factor p(say). This p obviously one of $p_1, p_2, \cdots p_n$. Now $p | p_1 p_2 \cdots p_n + 1, p | p_1 p_2 \cdots p_n$ together imply $p|1$ [Applying $x = -1, y = 1, b = p_1 p_2 \cdots p_n$ and $c = p_1 p_2 \cdots p_n + 1$ on $a|b, a|c \Rightarrow a|(bx + cy)$]. This leads to a contradiction (Why!). So our assumption is wrong and the theorem is proved. □

All the above results lead us to the fact that any integer can be factorized if it is composite. The factorized integers can be prime or composite such as $20 = 4 \times 5$ where 4 is composite whereas 5 is prime. But the most interesting fact is that $20 = 2^2 \times 5$ where both 2 and 5 are prime. This factorization is known to be prime factorization. The following Fundamental Theorem of Arithmetic or the unique factorization theorem enlighten us about the fact:

Theorem 3.2.5. *Every positive integer $n \geq 2$ can be expressed uniquely as product of primes, $n = p_1 p_2 p_3 \cdots p_r$, where each p_i is distinct for $1 \leq i \leq r$.*

Proof. If n is prime then we are done. If n is composite then there exists an integer d such that $d|n$ with $1 < d < n$. By well ordering principle, let p_1 be the smallest of them. Here p_1 must be prime otherwise t be any divisor of p_1 such that $1 < t < p_1$ then $t|p_1$ and $p_1|n$ together imply $t|n$ which is a contradiction(Why!). So we have $n = p_1 n_1$ for some integer n_1 where $1 < n_1 < n$. If n_1 is prime then we are done. If n_1 is composite then by the same argument we have another prime p_2 and integer n_2 where $1 < n_2 < n_1$ such that $n = p_1 p_2 n_2$. Continuing this way we have a decreasing sequence of integers $n > n_1 > n_2 > \cdots > 1$. This sequence is finite and after finite n_n we will get a prime p_r. This leads to prime factorization $n = p_1 p_2 \cdots p_r$.

To prove the uniqueness let there be two distinct prime factorizations of n as $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ where $r \leq s$ and each of $p_i' s$ and $q_j' s$ are primes. These primes are in the ordering $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq q_3 \leq \cdots \leq q_s$. As $p_1 | n$ this implies $p_1 | q_1 q_2 \cdots q_s$ then by virtue of Corollary 3.2.1 $p_1 = q_j$ for some j where $1 \leq j \leq n$. This follows that $p_1 < q_1$. Now cancelling the common factors from both the sides we have $q_2q_3\cdots q_s = p_2p_3\cdots p_r$. Continuing as above, up to r terms as $r < s$. After r-th step we have $1 = q_{r+1}q_{r+2}\cdots q_s$ which is absurd as $q_j's$ are prime. Hence $r = s$ and $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_s$. So the factorization is unique. $\square$

Let us consider an integer 15 which can be written as 5×3 where both 5 and 3 are distinct primes. But if we take 75 it can be expressed as $5\times 5\times 3$ where we can see the representation of primes. By collecting those primes and replacing them by a single factor we can represent any integer by following corollary viz

Corollary 3.2.2. *Any positive integer can be uniquely written as* $p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ *where each* n_i *is a positive integer and* $p_i's$ *are prime for* $i = 1, 2, 3, \ldots, r$ *with* $p_1 < p_2 < p_3 < \cdots < p_r$.

From the above corollary we can assert that any arbitrary positive integer has an unique prime factorization. Now in the later part of this section we have given an alternative proof of the Theorem 2.5.1. For that we have to define the greatest common divisor and least common multiple of any two arbitrary integers in the light of prime factorization. Let us take two integers a and b with their unique prime factorizations $a = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, $b = p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$ with $p_1 < p_2 < \cdots < p_n$ and a_k, b_k be non negative integers for $k = 1, 2, \cdots, n$. Then $\gcd(a, b) = p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}$ and $lcm(a, b) = p_1^{M_1}p_2^{M_2}\cdots p_n^{M_n}$ where $M_k = \text{Max}(a_k, a_k)$ and $m_k = \min(a_k, b_k)$. Here to give alternative proof of the Theorem 2.5.1 we first state and prove the lemma as follows:

Lemma 3.2.1. *If* x *and* y *are real numbers, then* $max(x, y) + min(x, y) = x + y$.

Proof. If $x < y$, then $\min(x, y) = x$ and $\max(x, y) = y$, and again we find that $\max(x, y) + \min(x, y) = x + y$. Similarly, If $x > y$, then $\min(x, y) = y$ and $\max(x, y) = x$, and again we find that $\max(x, y) + \min(x, y) = x + y$. $\square$

Now using the above lemma, let us proceed for the alternate proof:

Proof. Let a and b have prime-power factorizations $a = p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, $b = p_1^{b_1}p_2^{b_2}\cdots p_n^{b_n}$, where the powers are nonnegative integers and the primes $p_i's$ occurring in the prime-power factorizations of a and b. Let $M_k = \text{Max}(a_k, b_k)$

and $m_k = \min(a_k, b_k)$. Then, we have

$$\begin{aligned} lcm(a,b)\gcd(a,b) &= p_1^{M_1}p_2^{M_2}\cdots p_n^{M_n}p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n} \\ &= p_1^{M_1+m_1}p_2^{M_2+m_2}\cdots p_n^{M_n+m_n} \\ &= p_1^{a_1+b_1}p_2^{a_2+b_2}\cdots p_n^{a_n+b_n} \\ &= p_1^{a_1}p_1^{b_1}p_2^{a_2}p_2^{b_2}\cdots p_n^{a_n}p_n^{b_n} \\ &= ab. \end{aligned}$$

□

The numbers $2, 3, 4$ are integers and if we take $\frac{2}{3}, \frac{3}{4}$ then this type are the rational numbers of the form $\frac{p}{q}$ where $q \neq 0$ and $\gcd(p, q) = 1$. But there are numbers of the form $\sqrt{2}, \sqrt{3}$ which can not be written as above. These are said to be irrational numbers. We are now going to introduce a famous result of Pythagoras on irrational numbers viz

Theorem 3.2.6. *The number $\sqrt{2}$ is irrational.*

Proof. Let us suppose that $\sqrt{2}$ is a rational quantity. Then $\sqrt{2} = \frac{a}{b}$ where a, b are integers relatively prime to each other. Squaring we have, $2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$ implies $b^2 | a^2$. If $b > 1$, then by fundamental theorem of arithmetic we can say that there exists a prime p such that $p|b$. Then it follows $p|a^2$ implies $p|a$ and hence $\gcd(a, b) \geq p$ which is a contradiction unless $b = 1$. But if $b = 1$ holds then $a^2 = 2$ which is impossible(Why!). Hence the proof. □

For further discussion of this chapter we will show our interest in finding extremely large primes. To do so our first aim is to check whether a given integer is prime or not. We first deal with this question by trial division of n using the following theorem viz

Theorem 3.2.7. *If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.*

Proof. Since n is composite, we can write $n = ab$ where a, b are integers with $1 < a \leq b < n$. There must be $a \leq \sqrt{n}$, if not then $b \geq a > \sqrt{n}$ which leads to $ab > n$, which is not possible. Now from Theorem 3.2.3 the integer a must have a prime divisor p(say). Then $p \leq a \leq \sqrt{n}$. Further if $p|a$ and $a|n$ implies $p|n$. Then p is the required prime factor of n not exceeding $\sqrt{n}$. □

We can use this theorem to find all the primes less than or equal to a given positive integer n. This procedure is called Sieve of Eratosthenes. To illustrate the process, let us choose $n = 81$. Then by virtue of the above theorem, 81 has a prime factor less than or equal to $\sqrt{81} = 9$. Since, the only prime less than 9 are $2, 3, 5, 7$. We only have to find those integers less than 81 which can be divisible by any one of those primes. In the below table we have shown a complete list of them. The multiples of any one or two or three of $2, 3, 5, 7$ of the numbers in the table are cancelled by $/$, $\backslash$ and $\times$ respectively.

$\cancel{2}$	$\cancel{3}$	$\cancel{4}$	$\cancel{5}$	$\bcancel{6}$	$\cancel{7}$	$\cancel{8}$	$\cancel{9}$
$\bcancel{1}0$	11	$\bcancel{1}2$	13	$\bcancel{1}4$	$\bcancel{1}5$	$\cancel{1}6$	17
$\bcancel{1}8$	19	$\bcancel{2}0$	$\bcancel{2}1$	$\cancel{2}2$	23	$\bcancel{2}4$	$\cancel{2}5$
$\cancel{2}6$	$\cancel{2}7$	$\bcancel{2}8$	29	$\xcancel{3}0$	31	$\cancel{3}2$	$\cancel{3}3$
$\cancel{3}4$	$\bcancel{3}5$	$\bcancel{3}6$	37	$\cancel{3}8$	$\cancel{3}9$	$\cancel{4}0$	41
$\xcancel{4}2$	43	$\cancel{4}4$	$\bcancel{4}5$	$\cancel{4}6$	47	$\bcancel{4}8$	49
$\cancel{5}0$	$\cancel{5}1$	$\cancel{5}2$	53	$\bcancel{5}4$	$\cancel{5}5$	$\cancel{5}6$	$\cancel{5}7$
$\cancel{5}8$	59	$\bcancel{6}0$	61	$\cancel{6}2$	$\cancel{6}3$	$\cancel{6}4$	$\cancel{6}5$
$\bcancel{6}6$	67	$\cancel{6}8$	69	$\cancel{7}0$	71	$\cancel{7}2$	73
$\cancel{7}4$	$\cancel{7}5$	$\cancel{7}6$	$\cancel{7}7$	$\bcancel{7}8$	79	$\cancel{8}0$	$\cancel{8}1$

The above table indicates that there exist many primes less than 81. In fact, from theorem (3.2.4), we have infinitely many primes. A fairly natural question arises: Is it possible to estimate, how many primes are less than a positive real number x? We are fortunate enough to have the most renowned theorem of number theory, and of all mathematics, is the prime number theorem which answers this question. In 1793, Gauss speculated the theorem but it was an open problem until 1896, when a French mathematician J. Hadamard and a Belgian mathematician C. J. de la Vall*é*e-Poussin had proved it independently. So before going to state the theorem let us begin with a simple definition.

Definition 3.2.2. *The function $\pi(x)$, where x is a positive real number, denotes the number of primes not exceeding x.*

We now state the prime number theorem, whose proof is beyond the scope of the book.

Statement 3.2.1. *In language of limits, the theorem can be stated as* $\lim\limits_{x\to\infty} \dfrac{\pi(x)}{\ln x} = 1$.

The above stated theorem reflects the fact that for large values of x, $\dfrac{x}{\ln x}$ is a good approximation to $\pi(x)$. Further, it is to be noted that it is not necessary to find all primes not exceeding x in order to compute $\pi(x)$. By virtue of counting argument based on the Sieve of Eratosthenes,one can compute $\pi(x)$ without finding all the primes less than x.

Our next theorem addresses that the gap between consecutive primes is arbitrarily long.

Theorem 3.2.8. *For any positive integer n, there are at least n consecutive composite positive integers. Stated otherwise, there are arbitrarily large gaps in the series of primes.*

Proof. Consider the n consecutive positive integers

$$(n+1)!+2,(n+1)!+3,\ldots,(n+1)!+n+1.$$

Now, $2 \leq j \leq n+1 \Rightarrow j\big|(n+1)!$. Finally, an appeal to Proposition 2.2.1 yields the desired result. $\square$

The following example will exemplify our foregoing theorem.

Example 3.2.1. *For $n=5$, the smallest 5 consecutive composite integers can be found by locating the first pair of consecutive composite odd integers, 25 and 27. Hence the smallest 5 consecutive composite integers are $24,25,26,27,$ and 28. These are considerably smaller than the integers $(5+1)!+j=6!+j=720+j$ for $j=2,3,4,5,6$. Also, the seven consecutive integers beginning with $8!+2=40322$ are all composite. However, these are much larger than the smallest seven consecutive composites $90,91,92,93,94,95,$ and 96.*

Our next discussion is about the propagation of prime numbers of prime numbers. Let us choose p a prime and $\tilde{p}$ to be the product of all primes that are less than or equal to p. The numbers $\tilde{p}+1$ form are called "Euclidean numbers" as they appear in the proof of Theorem 3.2.4. For example,

$$\tilde{2}+1=2+1=3$$
$$\tilde{3}+1=2\cdot 3+1=7$$
$$\tilde{5}+1=2\cdot 3\cdot 5+1=31$$

are all prime numbers but also we can see $\widetilde{13}=59\cdot 509$ is not prime. From these two types of examples, we see that $\tilde{p}+1$ is not always a prime.

If we consider a sequence of integers such as,

$$\begin{aligned} n_1 &= 2 \\ n_2 &= n_1 + 1 \\ n_3 &= n_1 n_2 + 1 \\ &\vdots \\ n_k &= n_1 n_2 \cdots n_{k-1} + 1 \end{aligned}$$

where each $n_k > 1$ and they are relatively prime to each other. If not, let $\gcd(n_i, n_j) = d$ where $i < j$. Then $d|n_i \Rightarrow d\big|n_1 n_2 \cdots n_i \cdots n_{j-1}$. Since, $d\big|n_j$ therefore $d|n_1 n_2 \cdots n_{j-1} + 1$ together imply $d|1$, possible when $d = 1$. So our assertion, all $n_k' s$ are pairwise relatively prime, is true. Now we can say that there are many distinct primes as there are integers n_k.

Let p_n be n-th prime number. Then from Euclid's proof we can estimate the rate of increase of p_n. Here we have $p_{n+1} \leq p_1 p_2 \cdots p_n + 1 < p_n^n + 1$. If $n = 5$ then $31 = p_6 = p_5^5 + 1 = 7^5 + 1 = 16808$. Thus we have the following theorem viz

Theorem 3.2.9. *If p_k be the k-th prime, then $p_k \leq 2^{2^k - 1}$.*

Proof. We will prove the theorem by Mathematical Induction on k. If $k = 1$, then the result is obvious. Let us assume $k > 1$. Then

$$\begin{aligned} p_{k+1} &\leq p_1 p_2 \cdots p_k + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{k-1} + 1 = 2^{1+2+2^2+\cdots+2^{k-1}} + 1 = 2^{2^k - 1} + 1. \end{aligned}$$

But $1 \leq 2^{2^k - 1}$ for all k. Therefore $p_{k+1} \leq 2^{2^k}$ (How!). Thus the result is true for $k + 1$. Hence the proof. □

The last inequation of the above proof gives rise to an interesting corollary stated as follows:

Corollary 3.2.3. *For $k \geq 1$ there exists at least $k + 1$ primes less than 2^{2^k}.*

Proof. left to the reader. □

Finally, we conclude this section with remarkable conjecture about primes, commonly known as Golbach's Conjecture, stated by Christian Goldbach in a letter to Euler in 1742.

Goldbach Conjecture: Every even positive integer greater than two can be written as the sum of two primes.

Let us exemplify the Conjecture with an example:

$$\begin{aligned}10 &= 3+7=5+5\\24 &= 5+19=7+17=11+13\\100 &= 3+97=11+89=17+83\\&= 29+71=41+59=47+53\end{aligned}$$

Next with the help of the following lemma, we are going to prove the fact that there exists infinitely many primes of the form $4n+3$.

Lemma 3.2.2. *The product of two or more integers of the form* $4n+3$ $(n \in \mathbb{Z})$ *results in the same form.*

Proof. It's sufficient to prove the lemma with two integers of the form $4n+1$. Set $k_1 = 4n_1+1,\ k_2 = 4n_2+1$. Multiplying we obtain,

$$\begin{aligned}k_1k_2 &= (4n_1+1)(4n_2+1)\\&= 4(4n_1n_2+n_1+n_2)+1\\&= 4n+1,\ [n = 4n_1n_2+n_1+n_2 \in \mathbb{Z}]\end{aligned}$$

which is the desired form. □

This facilitates the proof for the following theorem.

Theorem 3.2.10. *There exists infinitely many primes of the form* $4n+3$.

Proof. Suppose there exists finitely many primes $t_1, t_2, \ldots, t_s$ of the form $4n+3$. Also, consider $N = 4t_1t_2\ldots t_s - 1 = 4(t_1t_2\ldots t_s - 1) + 3$ to be a positive integer. Further, let $N = k_1k_2\ldots k_n$ be the prime factorization of N. Since N is odd, then $k_i \neq 2,\ \forall\, i$. Thus k_i is of the form, either $4n+1$ or $4n+3$. If k_i is of the form $4n+1$, then using the lemma 3.2.2 we can say that N must be of the form $4n+1$. This is not the case here. Then N must contain one prime factor k_i of the form $4n+3$. But, k_i can not be found among $t_1, t_2, \ldots, t_s$. Otherwise this leads to $k_i | 1$, which is not true. Thus our assumption of finitely many primes of the form $4n+3$ is wrong. □

The last theorem inspired us to ask a fairly question: Is the number of primes of the form $(4n+1)$ also infinite? The following Dirichlet's statement, whose proof is beyond the scope of the book, is the answer to the question.

Theorem 3.2.11. *If a and b are positive integers with $\gcd(a,b)=1$, then the arithmetic progression*

$$a, a+b, a+2b, \ldots$$

contains infinite number of primes.

From Dirichlet's statement it can be seen that there exists infinitely many primes ending with 999, for instance 1999, 1000999, . . ., they appear in arithmetic progression given by $1000n+999$, with $\gcd(1000,999)=1$.

Theorem 3.2.12. *There exists no arithmetic progression of the form $a, a+b, a+2b, \ldots$ that consists of only primes.*

Proof. To begin with, consider $a+nb=p$, p being a prime. If $n_k=n+kp$ for $k=1,2,3\ldots$ then the n_k-th term in the progression is

$$\begin{aligned} a+n_kb &= a+(n+kp)b \\ &= (a+nb)+kbp = p+kbp \\ &= p(1+kb) \end{aligned}$$

Since, $p|p(1+kb)$, therefore $p|(a+n_kb)$. Hence $(a+n_kb)$ can not be a prime, which is our desired result. ☐

Remark 3.2.1. *From the above theorem, it's quite clear that the progression contains infinitely many composite numbers.*

Theorem 3.2.13. *If all the $n(>2)$ terms of the arithmetic progression,*

$$p, p+d, p+2d, \ldots$$

are primes, then $q|d$ where d being the common difference and $q(<n)$ is a prime number.

Proof. Consider a prime $q<n$. In anticipation of a contradiction, assume $q\nmid d$. Again, if possible let us assume that the first q terms of the given progression will leave the same remainders when divided by q. Then $\exists j,k\in\mathbb{Z}$ with $0\le j<k\le q-1$ or $k-j\le q-1$ such that $(p+jd)$ and $(p+kd)$ generates same remainder when divided by q, which further implies $q\big|(k-j)$. But $\gcd(p,q)=1$ and by Euclid's lemma $q\big|(k-j)$, which is impossible in the light of the inequality $k-j\le q-1$. Hence the first q terms of the given progression will leave q different remainder upon division by q. Since they are extended from q integers $0,1,2,\ldots,q-1$, one of them must be zero.This means for some t satisfying $0\le t\le q-1$, $q|(p+td)$. Hence we conclude, $p+td$ is composite because the inequality $q<n\le p\le(p+td)$ holds (for if $p\le n$, then one of the term of the progression will be $p(1+d)$). This leads to a contradiction and hence $q\big|d$. ☐

Remark 3.2.2. *There is a conjecture that there exists arithmetic progression of finite length, consisting of consecutive prime numbers. For instance,* $47, 53, 59$ *and* $251, 257, 263, 269$.

Consider the function $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ defined by $f(n) = n^2 + n + 41$. There was a myth that the image set of the function was only primes. But in 1772, it was proved to be false by Leonhard Euler. Though the myth was true for $n = 0, 1, 2 \ldots, 39$ but fails for $n = 40, 41$. Here

$$\begin{aligned} f(40) &= 40 \cdot 41 + 41 = 41^2, \quad \text{and} \\ f(41) &= 41 \cdot 42 + 41 = 41 \cdot 43. \end{aligned}$$

Once again $f(42) = 1847$ turns out to be prime. The polynomial $f(n) = (n^2 + n + 41)$ is known as Euler polynomial. It is to be noted that no polynomial of the form $n^2 + n + q$, q being prime, can perform better than Euler polynomial in giving primes for successive values of n.

Theorem 3.2.14. *There exists no non-constant polynomial* $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ *with integral coefficients that generates solely prime numbers for* $n \in \mathbb{Z}^+$.

Proof. To the contrary, assume that such a polynomial f does exists. Set $f(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots + a_2 n^2 + a_1 n + a_0$ where the coefficients $a_i (i = 0, 1, 2 \ldots, k)$ are integers with $a_k \neq 0$. Let $f(n_0) = p$, for some fixed value $n_0 \in \mathbb{Z}^+$. Now, for any $t \in \mathbb{Z}$, consider

$$\begin{aligned} f(n_0 + tp) &= a_k(n_0 + tp)^k + a_{k-1}(n_0 + tp)^{k-1} + \ldots + a_2(n_0 + tp)^2 + a_1(n_0 + tp) + a_0 \\ &= (a_k n^k + a_{k-1} n^{k-1} + \ldots + a_2 n^2 + a_1 n + a_0) + pQ(t) \\ &= f(n_0) + pQ(t) \\ &= p(1 + Q(t)), \end{aligned}$$

$Q(t)$ being a polynomial in t with integral coefficients. This shows $p | f(n_0 + tp)$, which further implies $f(n_0 + tp) = p$ $(t \in \mathbb{Z})$. This leads to a contradiction(Why!).Thus we have established the theorem. □

3.3 Worked out Exercises

Problem 3.3.1. *The lucky numbers are generated by the screening process as follows: Let us begin with the set of positive integers. Starting the process by crossing out every second integer in the list, start the count with the integer* 1. *Other than* 1 *the smallest integer left is* 3*, continuing with the process every third integer left, beginning with the integer* 1. *The next integer left is* 7*, so we cross* *out every seventh integer left. Continuing as above, where at each stage we cross out every κth integer left where κ is the smallest integer left other than one. The integers that remain are the lucky numbers. Prove that the lucky number set is countably infinite.*

Solution 3.3.1. *At each stage of the procedure for generating the lucky numbers the smallest number left is κ, say, is designated to be a lucky number and infinitely many primes are left after the deletion of every κ integer left. It follows that there are countably infinite numbers of steps, and at every step a new lucky number is added to the sequence. Hence the proof.*

Problem 3.3.2. *Show that the polynomial $f(x) = x^2 - x + 41$ is prime for all integers x with $0 \leq x \leq 40$. Furthermore, it is composite for $x = 41$.*

Solution 3.3.2. *Hint: Find $f(1), f(2), f(3), \ldots, f(39), f(40)$. But $f(41)$ is composite.*

Problem 3.3.3. *Show that if $g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ where the coefficients are integers, then $\exists\, y \in \mathbb{Z}$ such that $g(y)$ is composite.*

Solution 3.3.3. *In anticipation to contradiction, suppose there $\nexists$ any $y \in \mathbb{Z}$ such that $g(y)$ is composite. Let y_0 be a positive integer such that $g(y_0) = p$, a prime. Let κ be any integer such that $g(y_0 + \kappa p) = a_n (y_0 + \kappa p)^n + a_{n-1}(y_0 + \kappa p)^{n-1} + \cdots + a_1 (y_0 + \kappa p) + a_0$. By binomial expansion it follows that $g(y_0 + \kappa p) = \sum_{j=0}^{n} a_j x_0^j + Mp$, M being an integer. Now $p | (g(y_0 + Mp) = g(y_0 + \kappa p)$ (Why!). Also $g(y_0 + \kappa p) = p$ (Why!). This contradicts the fact that a polynomial of degree n takes on each value not more than n times. Hence there is an integer y such that $g(y)$ is composite.*

Problem 3.3.4. *Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.*

Solution 3.3.4. *Note that n must be positive. Otherwise no such integers are prime (Why!). Since $n^3 + 1 = (n+1)(n^2 - n + 1)$, $n^3 + 1$ is not prime unless one of the two factors on the right hand side of the equation is 1 and the other is $n^3 + 1$. But $(n + 1) > 1$ for every positive integer n and the only way for $n + 1 = n^3 + 1$ is when $n = 1$(Verify!). In this case, we have $1^3 + 1 = (1 + 1)(1^2 - 1 + 1) = 2$. Hence 2 is the only prime of this form.*

Problem 3.3.5. *Find all primes that are the difference of the fourth powers of two integers.*

Solution 3.3.5. *Suppose* $n = a^4 - b^4 = (a-b)(a+b)(a^2+b^2)$, *where* $a > b$. *The integer* n *cannot be prime because it is divisible by* $a+b$ *which cannot be* 1 *or* n.

Problem 3.3.6. *Show that if* a *and* n *are positive integers such that* $a^n - 1$ *is prime, then* $a = 2$ *and* n *is prime.*

Solution 3.3.6. *Let* n *be a composite number and* k *be any divisor of* n. *Then* $1 < k < n$ *and* $(a^k - 1)|(a^n - 1)$. *As* $a^n - 1$ *is prime, so* $a^k - 1 = 1$*(Why!). This is true, if* $a = 2$ *and* $k = 1$. *This leads to a contradiction as* $k > 1$. *Thus we have* $a = 2$ *and* n *is prime.*

Problem 3.3.7. *Show that every integer greater than* 11 *is the sum of two composite integers.*

Solution 3.3.7. *Let us assume that* n *be an integer greater than* 11.

Case I n *is even: Then there exists an integer* k *such that* $n = 2k$. *Since* $n > 11$, *therefore* $n \geq 12$ *and thus* $k \geq 6$. *Now* $n - 4 = 2(k-2)$ *with* $k - 2 \geq 4$. *By definition of divisibility, we have* $2|(n-4)$ *and* $(k-2)|(n-4)$. *By definition of compositeness,* $n - 4$ *is composite. Also* $n = (n-4) + 4$. *As* 4 *is composite, therefore* n *is the sum of two composite numbers.*

Case II n *is odd: Then there exists an integer* k *such that* $n = 2k+1$. *Since* $n > 11$, *therefore* $n \geq 13$ *and thus* $k \geq 6$. *Now* $n - 9 = 2(k-4)$ *with* $k - 4 \geq 2$. *By definition of divisibility, we have* $2|(n-9)$ *and* $(k-4)|(n-9)$. *Again by definition of compositeness, we have* $n - 9$ *is composite. Also* $n = (n-9)+9$. *As* 9 *is composite, therefore* n *is the sum of two composite numbers.*

Problem 3.3.8. *If* $p \geq 5$ *is a prime number, show that* $p^2 + 2$ *is composite.*

Solution 3.3.8. *By division algorithm,* $p = 6q + r$ *where* $r = 0, 1, 2, 3, 4, 5$.

Case i: *If* $r = 0$, *then* $p = 6q$ *implies* $6|p$, *a contradiction(Why!). Hence* $r \neq 0$

Case ii: *If* $r = 2$, *then* $p = 6q + 2$ *implies* $2|p$, *a contradiction. Hence* $r \neq 2$

Case iii: *If* $r = 3$, *then* $p = 6q + 3$ *implies* $3|p$, *a contradiction. Hence* $r \neq 3$

Case iv: *If* $r = 4$, *then* $p = 6q + 4$ *implies* $2|p$, *a contradiction. Hence* $r \neq 4$

Thus $r = 1, 5$ *implies* $p = 6q + 1$ *or* $p = 6q + 5$. *Therefore* $3|(p^2 + 2)$ *in either case(Why!). Hence the proof.*

Problem 3.3.9. *If* $p \neq 5$ *is an odd prime, prove that either* $p^2 - 1$ *or* $p^2 + 1$ *is divisible by* 10.

Solution 3.3.9. *Here* p *is of the form:* $10q+1, 10q+3, 10q+7, 10q+9$. *But* $p \neq 10q+$ *even since it can factor out* 2*, so fails to be prime. Now,*

$$\begin{aligned}
(10q+1)^2 &= 100q^2 + 20q + 1 \Rightarrow 10|(p^2-1)\\
(10q+3)^2 &= 100q^2 + 60q + 9 \Rightarrow 10|(p^2+1)\\
(10q+7)^2 &= 100q^2 + 140q + 49 \Rightarrow 10|(p^2+1)\\
(10q+9)^2 &= 100q^2 + 180q + 81 \Rightarrow 10|(p^2-1).
\end{aligned}$$

Problem 3.3.10. *If* $n > 1$ *is an integer not of the form* $6k+3$*, prove that* $n^2 + 2^n$ *is composite.*

Solution 3.3.10. *Here* n *is of the form* $6q, 6q+1, 6q+2, 6q+4, 6q+5$.

Case (i): *When* $n = 6q$*, then* $n^2 + 2^n = 36q^2 + 2^{6q} \Rightarrow 2|(36q^2 + 2^{6q})$ *as* $q > 0$*, hence a composite number.*

Case (ii): *When* $n = 6q+1$*, then* $n^2 + 2^n = 36q^2 + 12q + 2^{6q+1} + 1 = 36q^2 + 12q + (2+1)(2^{6q} - \cdots + (-1)^{6q}1^{6q})(Why!) \Rightarrow 3|(n^2+2^n)$*, hence a composite number.*

Case (iii): *When* $n = 6q+2$*, then* $n^2+2^n = 36q^2+24q+4+2^2 2^{6q} \Rightarrow 2|(n^2+2^n)$*, hence a composite number.*

case (iv): *When* $n = 6q+4$*, then* $n^2+2^n = 36q^2+48q+16+2^4 2^{6q} \Rightarrow 2|(n^2+2^n)$*, hence a composite number.*

Case (v): *Treated as an exercise.(Hint! Similar to* $6q+1$ *as above.)*

Problem 3.3.11. *Prove that a positive integer* $a > 1$ *is a square if and only if in the prime factorizations of* a *all the exponents of the primes are even integers.*

Solution 3.3.11. *Let* $a > 1$ *be square. Then* $a = n^2$*, for some integer* n*. Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$*. Therefore* $n^2 = p_1^{2k_1} p_2^{2k_2} \cdots p_s^{2k_s}$ *shows all exponents are even.*

Conversely, suppose all exponents of $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ *are even. Therefore* $k_i = 2m_i$ *for some* m_i *and for every* k_i*. Therefore* $a = p_1^{2m_1} p_2^{2m_2} \cdots p_s^{2m_s} = (p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s})^2$.

Problem 3.3.12. *An integer is said to be square-free if it is not divisible by the square of any integer greater than* 1*. Prove the following:*

1. *An integer $n > 1$ is square-free if and only if n can be factored into a product of distinct primes.*
2. *Every integer $n > 1$ is the product of a square-free integer and a perfect square.*

Solution 3.3.12. *1. Let $n > 1$ be square free and $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ be the prime factorization of it. Then $k_i \geq 2$ and therefore $p_i^2 | n$, a contradiction to the definition of square free. Therefore $k_i = 1$. Hence $n = p_1 p_2 p_3 \cdots p_s$ with $p_i \neq p_j$. If possible, let n be not a square free and $a^2 | n$. Hence $n = la^2$, for some $l \in \mathbb{Z}$. Let $a = q_1^{k_1} q_2^{k_2} q_3^{k_3} \cdots q_r^{k_r}$. Therefore $p_1 p_2 p_3 \cdots p_s = l q_1^{2k_1} q_2^{2k_2} q_3^{2k_3} \cdots q_r^{2k_r}$ implies $q_j | p_1 p_2 p_3 \cdots p_s$. By virtue of Corollary (3.2.1), $q_j = p_i$ for some $i = 1, 2, 3, \ldots, s$. After factoring out q_j and p_i, we still have $p_1 p_2 p_3 \cdots p_s = l q_1^{2k_1} q_2^{2k_2} q_3^{2k_3} \cdots q_r^{2k_r}$ implies $q_j | p_1 p_2 p_3 \cdots p_s$. But the original factorization $p_1 p_2 p_3 \cdots p_s$ was unique and q_j was factored out. Hence q_j fails to divide the remaining factorization, which shows n to be square free.*

2. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ be the prime factorization of it. If k_i is odd and $k_i > 1$, then $k_i - 1$ is even. Let $a = p_{r_1}^{k_{r_1}} p_{r_2}^{k_{r_2}} \cdots p_{r_m}^{k_{r_m}}, 1 \leq r_i \leq s$ and k_{r_i} is odd with $k_{r_i} \geq 1$. Let $b = p_{r_1} p_{r_2} \cdots p_{r_m}$. Then $a = b p_{r_1}^{k_{r_1} - 1} p_{r_2}^{k_{r_2} - 1} \cdots p_{r_m}^{k_{r_m} - 1}$. Also b is square free(Why!). Since $k_{r_i} - 1$ is even, $p_{r_i}^{k_{r_i} - 1} = p_{r_i}^{2l_i}$. Let $c = p_{r_1}^{l_1} p_{r_2}^{l_2} \cdots p_{r_m}^{l_m}$. Then, $a = bc^2$. Finally, suppose $a | n = p_{l_1}^{k_{l_1}} p_{l_2}^{k_{l_2}} \cdots p_{l_j}^{k_{l_j}}$ where all k_{l_j} are even as $a | n$ has factored out all of the odd exponents in the canonical form of n. By previous problem above, $a | n = d^2 \Rightarrow n = bc^2 d^2 = b(cd)^2$, where b is square free.

Problem 3.3.13. *Find all prime numbers that divide* 50!.

Solution 3.3.13. *All primes less than* 50 *will divide* 50! *because each is a term of* 50!. *By the fundamental theorem of Arithmetic, each term k of* 50! *that is non–prime has a unique prime factorization. And each term of the unique factorization of k is smaller than k, so is prime less than* 50. *There is no prime greater than* 50 *represented in this factorization of k. Hence all primes less than* 50 *will divide* 50!.

Problem 3.3.14. *Show that any composite three-digit number must have a prime factor less than or equal to* 31.

Solution 3.3.14. *We know* 999 *is the largest composite three digit number. Now $\sqrt{999} = 31.6$. Here* 31 *is prime, so if a is composite, largest prime divisor is less than equal to $\sqrt{a}$. Hence* 31 *is largest possible prime divisor.*

Problem 3.3.15. *Prove that the prime number set is countably infinite using the integer* $N = p! + 1$.

Solution 3.3.15. *Let us assume there are finitely many primes,* p_n *being the largest. Then* $N = p_n! + 1 = 1 \cdot 2 \cdots p_n + 1$. *Now* N *must have a prime divisor* p_k *with* $1 \leq k \leq n$*(Why!). And* $p_k | 1 \cdot 2 \cdots p_n$ *(Why!). Therefore* $p_k | (N - 1 \cdot 2 \cdots p_n) \Rightarrow p_k | 1 \Rightarrow p_k = 1$*, a contradiction.*

Problem 3.3.16. *Any integer* n *can be expressed as* $n = 2^k m$*, where* $k \geq 0$ *and* m *being an odd integer. Verify!*

Solution 3.3.16. *With out any loss of generality, assume* $n > 0$*, for if* $n < 0$ *then* $-n = 2^k m \Rightarrow n = 2^k(-m)$. *Now the following cases will arise:*

Case(i) *If* n *is odd, then* $k = 0$ *and* $m = n$.

Case(ii) *If* n *is even, then* $n = 2k_1, k_1 < n$.

Case(iii) *If* k_1 *is odd, then we are done.*

Case(iv) *If* k_1 *is even, then* $k_1 = 2k_2$ *so* $n = 2^2 k_2$ *where* $k_2 < k_1 < n$.

Continuing as above after i-th stage we have $2^i k_i$*, where* $k_i < k_{i-1}$. *This is a finite process and after a certain stage we will reach at* $k_t = 1$ *and there will be no odd integer after* 1. *In that stage,* $n = 2^t k_t = 2^t \cdot 1$. *Thus* n *can be expressed as* $n = 2^k m$*, where* $k \geq 0$ *and* m *being an odd integer.*

Problem 3.3.17. *Prove or Disprove: Every positive integer can be written in the form* $p + a^2$*, where* p *is either a prime or* 1*, and* $a \geq 0$.

Solution 3.3.17. *Hint:* $25 = p + a^2$ *then consider* $a = 1, 2, 3, 4, 5$.

Problem 3.3.18.

1. *Prove: Any prime of the form* $3n+1$ *is also of the form* $6m + 1$.
2. *The only prime of the form* $n^3 - 1$ *is* 7.

Solution 3.3.18.

1. *Here* $p = 3n + 1$ *is prime implies* p *is odd. Then* $p - 1 = 3n$ *is even implies* n *is even. Hence* $n = 2m$*, for integer* m. *Thus* $3n + 1 = 6m + 1$.
2. *Here* $t = n^3 - 1 = (n - 1)(n^2 + n + 1)$. *If* $n = 1$*, then* t *is prime. If* $n = 2, t = 7$. *If* $n > 2$*, then* t *will be a factor of two integers, neither of which is* 1. *Hence for* $n > 2$*,* t *can't be prime.*

Problem 3.3.19. *Find five primes of the form* $n^2 - 2$.

Solution 3.3.19. *Hint: Consider* $n = 2, 3, 5, 7, 9$.

Problem 3.3.20. *A positive integer* n *is said to be square-full, or powerful, if* $p^2|n$ *for every prime factor* p *of* n. *Prove that if* n *is square-full, then it can be written in the form* $n = a^2b^3$, *with* a *and* b *positive integers.*

Solution 3.3.20. *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *be the prime factorization of it. Since* n *is square-full,* $k_i \geq 2$. *Listing first the odd exponents and then the even one, let us assume*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} = q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} q_{n_1}^{k_{n_1}} q_{n_2}^{k_{n_2}} q_{n_3}^{k_{n_3}} \cdots q_{n_t}^{k_{n_t}},$$

where k_{m_i} *are odd(so* $k_{m_s} \geq 3$*) and* k_{n_i} *are even. Therefore for some* v_i, $k_{n_i} = 2v_i$. *Therefore*

$$\begin{aligned} n &= q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} (q_{n_1}^{2v_1} q_{n_2}^{2v_2} q_{n_3}^{2v_3} \cdots q_{n_t}^{2v_t}) \\ &= q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} (q_{n_1}^{v_1} q_{n_2}^{v_2} q_{n_3}^{v_3} \cdots q_{n_t}^{v_t})^2. \\ \textit{Hence, } n &= q_{m_1}^{k_{m_1}} q_{m_2}^{k_{m_2}} q_{m_3}^{k_{m_3}} \cdots q_{m_s}^{k_{m_s}} (Y)^2, Y = q_{n_1}^{v_1} q_{n_2}^{v_2} q_{n_3}^{v_3} \cdots q_{n_t}^{v_t}. \end{aligned}$$

Now k_{m_i} *is odd and* ≥ 3 *together implies* $k_{m_i} - 3$ *is even. Thus*

$$n = q_{m_1}^3 q_{m_2}^3 q_{m_3}^3 \cdots q_{m_s}^3 (q_{m_1}^{m_1 - 3} q_{m_2}^{m_2 - 3} q_{m_3}^{m_3 - 3} \cdots q_{m_s}^{m_s - 3})(Y)^2.$$

Let $m_i - 3 = 2w_i, q_{m_1} q_{m_2} q_{m_3} \cdots q_{m_s} = b$. *Therefore*

$$n = b^3(q_{m_1}^{2w_1} q_{m_2}^{2w_2} q_{m_2}^{2w_3} \cdots q_{m_s}^{2w_s})(Y^2).$$

Let $X = q_{m_1}^{w_1} q_{m_2}^{w_2} q_{m_{w_3}}^{3} \cdots q_{m_s}^{w_s}$. *Then* $n = b^3X^2Y^2$. *Taking* $a = XY$, *we obtain* $n = a^2b^3$.

Problem 3.3.21. *Given that* $p \nmid n$ *for all primes* $p \leq \sqrt[3]{n}$, *prove that* $n > 1$ *is either a prime or the product of two primes.*

Solution 3.3.21. *Assuming* n *to be composite and taking* $n = p_1 p_2 \cdots p_X$ *with* $X \geq 3$, *we know that*

$$1 < \sqrt[3]{n} < p_i \leq \sqrt{n}.$$

Therefore

$$\begin{aligned} \sqrt[3]{n} &\leq p_1 \leq \sqrt{n} \\ \sqrt[3]{n} &\leq p_2 \leq \sqrt{n} \\ \sqrt[3]{n} &\leq p_3 \leq \sqrt{n}. \end{aligned}$$

Therefore $n = (\sqrt[3]{n})(\sqrt[3]{n})(\sqrt[3]{n}) < p_1 p_1 p_2 p_3 = n \Rightarrow n < n$. *Hence* $X < 3$ *or* $= 2$ *or* $= 1$. *Thus* $n > 1$ *is either a prime(*$X = 1$*) or the product of two primes(*$X = 2$*).*

Problem 3.3.22. *Prove that if* $n > 2$, *then there exists a prime* p *satisfying* $n < p < n!$.

Solution 3.3.22. *For* $n > 2$,

$$n < n! - 1 < n!.$$

If $n! - 1$ *is prime, we are done. If* $n! - 1$ *is not prime, taking* p *to be a prime divisor, we have* $p < n! - 1$. *Suppose* $p \leq n$. *Then* p *is one of the terms in* $1, 2, 3, \ldots, n$. *So* $p|n!$. *Therefore* $p|n!$ *and* $p\big|(n! - 1)$ *together implies* $p\big|\big(n! - (n! - 1)\big) = 1$. *Therefore* $p > n$ *and hence the result.*

Problem 3.3.23. *For* $n > 1$, *show that every prime divisor of* $n! + 1$ *is an odd integer that is greater than* n.

Solution 3.3.23. *Because* $n!$ *is even for* $n > 1$, *therefore* $n! + 1$ *is odd. Hence* $2 \nmid (n! + 1)$, *so every prime divisor of* $n! + 1$ *is odd.*

Suppose every prime divisor p_i *of* $n! + 1$ *is less than or equal to* n. *Since* p_i *is one of the members of* $n!$, *therefore* $p_i|n!$. *Also* $p_i|(n! + 1) \Rightarrow p_i|(n! + 1) - n! = 1$, *a contradiction. Thus* p_i *is greater than* n.

Problem 3.3.24. *If* a *is a positive integer and* $\sqrt[n]{a}$ *is rational, then* $\sqrt[n]{a}$ *is an integer.*

Solution 3.3.24. *Let* $\sqrt[n]{a} = \dfrac{r}{s}$, *where* r, s *being integers and* $\gcd(r, s) = 1$ *with* $s \neq 0$. *Let* $r = p_1 p_2 \cdots p_X$, $s = q_1 q_2 \cdots q_Y$. *Then* $p_i \neq q_j$. *Therefore*

$$(q_1 q_2 \cdots q_Y)^n a = (p_1 p_2 \cdots p_X)^n.$$

Therefore $(p_1 p_2 \cdots p_X)^n | a$. *Let* $a = (p_1 p_2 \cdots p_X)^n t$, *for some integer* t. *Therefore*

$$(q_1 q_2 \cdots q_Y)^n (p_1 p_2 \cdots p_X)^n t = (p_1 p_2 \cdots p_X)^n,$$

implies $q_j = 1$ *for all* j. *Thus* $s = 1$ *and* $\dfrac{r}{s} = \sqrt[n]{a}$, *an integer.*

Problem 3.3.25. *Prove for* $n \geq 2$, $\sqrt[n]{n}$ *is irrational.*

Solution 3.3.25. *Suppose,* $n \geq 2$, $\sqrt[n]{n}$ *is rational. Then by Problem 3.3.24, it is an integer. Let* $\sqrt[n]{n} = a$. *Then* $n = a^n$. *But* $n < 2^n \Rightarrow a^n < 2^n \Rightarrow$ *either* $a < 2$ *or* $a = 1$. *Therefore* $n = 1^n = 1$, *a contradiction.*

Problem 3.3.26. *Prove that any odd prime* p *is of the form* $4k + 1$ *or* $4k + 3$ *for any non-negative integer* k.

Solution 3.3.26. *By Division Algorithm, any positive integer can be expressed in the form* $a = bq + r,\ 0 \leq r < b$ *or equivalently written as* $a = 4q + r,\ r = 0, 1, 2, 3$. *Now if;*

$$r = 0, a = 4q = 2(2q),\ \textit{an even integer.}$$

$$r = 1, a = 4q + 1 = 2(2q) + 1,\ \textit{an odd integer.}$$

$$r = 2, a = 4q + 2 = 2(2q) + 2 = 2(2q + 1) = 2m, \textit{an even integer.}$$

$$r = 3, a = 4q = 2(2q) + 3 = 2(2q + 1) + 1 = 2m + 1, \textit{an odd integer.}$$

Hence any odd prime p *is of the form* $4k + 1$ *or* $4k + 3$ *for any non-negative integer* k.

Problem 3.3.27. *If* p *and* $p^2 + 8$ *are both prime numbers, prove that* $p^3 + 4$ *is also prime.*

Solution 3.3.27. *Referring to Problem 3.3.8, if* $p > 3$ *is prime, it is of the form* $(6k + 1)$ *or* $(6k + 5)$. *So for* $p = 6k + 1$ *or* $6k + 5$, *we have* $p^2 + 8 = 36k^2 + 12k + 9$ *or* $p^2 + 8 = 36k^2 + 60k + 33$ *respectively. But* $3\big|(36k^2 + 12k + 9)$ *and* $3\big|(36k^2 + 60k + 33)$. *So* $p^2 + 8$ *is not prime, provided* $p > 3$. *By the problem, both* p *and* $p^2 + 8$ *are primes. Thus the only possibility is* $p = 3$, *which yields* $p^2 + 8 = 17$. *Hence* $p^3 + 4 = 31$.

Problem 3.3.28. *Bertrand Conjecture: For any positive integer* z, $\exists$ *a prime* p *satisfying* $z \leq p < 2z$. *Using this proves that for every* $n \geq 2$, $\exists$ *a prime* p *with* $p < n < 2p$.

Solution 3.3.28. ***Case-I:*** *n is odd: Since* $n \geq 2$ *&* $k \geq 1$, $\exists\ k \in \mathbb{Z}$ *such that* $n = 2k + 1$. *Addressing to Bertrand's Conjecture,* $\exists$ *a prime* p *satisfying* $k < p < 2k$. *Now* $p < (p + 1) < (2k + 1) = n \Rightarrow p < n$. *Further* $2k < 2p \Rightarrow (2k+1) \leq 2p \Rightarrow n \leq 2p$. *But* $(2k+1)$ *being odd and* $2p$ *is even, together conclude* $n < 2p$. *Thus* $\exists$ *a prime* p *such that* $p < n < 2p$.

Case-II: *n is even: Since* $k \geq 1$, $\exists\ k \in \mathbb{Z}$ *such that* $n = 2k$ *holds. An appeal to Bertrand's Conjecture yields,* $k < p < 2k = n \Rightarrow p < n$*(p being a prime). Therefore* $n = 2k < 2p \Rightarrow n < 2p$. *Thus* $p < n < 2p$.

Problem 3.3.29. *Let* p_n *denote the n-th prime number. For* $n \geq 3$, *prove that* $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$.

Solution 3.3.29. *Note that* $p_{n+1} < 2p_n$. *Therefore* $p_{n+3} < 2p_{n+2}$. *So* $p_{n+3}^2 < 4p_{n+2}^2 < 4p_{n+2}(2p_{n+1}) = 8p_{n+2}p_{n+1}$. *Now* $p_5 = 11 \Rightarrow 8p_{n+2}p_{n+1} < p_5 p_{n+2} p_{n+1}$. *Therefore* $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$, *if* $n \geq 5$.

For $n = 4$; $p_7^2 = 289 < p_4 p_5 p_6 = 1001$. *For* $n = 3$; $p_6^2 = 169 < p_3 p_4 p_5 = 385$. *For* $n = 2$; $p_5^2 = 121 < p_2 p_3 p_4 = 105$. *Hence for* $n \geq 3$, $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$.

Problem 3.3.30. *There exist infinitely many primes that do not belong to any pair of twin primes.*

Solution 3.3.30. *Here* $\gcd(5,21)=1$*. By Dirichlet's theorem, the series* $5+21k$ *for* $k=1,2,3,\ldots,$ *contains infinitely many primes. Let* p *be one such prime. Then* $p=5+21k(k\in\mathbb{Z})$ *gives* $p+2=7(1+3k)$ *and* $p-2=3(1+7k)$*. Thus* $(p+2)$ *and* $(p-2)$ *fails to be prime. Hence all the primes contained in* $(5+21k)$ *cannot be numbers of twin primes.*

Problem 3.3.31. *Prove that there are infinitely many primes of the form* $6n+5$*.*

Solution 3.3.31. *To the contrary, assume only a finite number of primes of the form* $(6n+5)$*. Let this be* $q_1,q_2,\ldots,q_s$*. Consider* $N=6q_1q_2\ldots q_s-1=6(q_1q_2\ldots q_s-1)+5$*. Let* $N=r_1r_2\ldots r_t$ *be its prime factorization. Since* N *is odd,* $r_i\neq 2$ *for each* i*, so each* r_i *can only be of the form* $6n+1$*,* $6n+3$ *or* $6n+5$*. Since*

$$\begin{aligned}(6n+1)(6m+1)&=36mn+6m+6n+1\\&=6(6mn+m+n)+1\\&=6k+1,\quad \textit{where } k=(6mn+m+n),\end{aligned}$$

this shows the product of two integers of the form $(6n+1)$ *is of the same form. By similar reasoning, the product of two integers of the form* $(6n+3)$ *is also so. Furthermore,*

$$\begin{aligned}(6n+1)(6m+3)&=6(6mn+m+3n)+3\\&=6k'+3,\quad \textit{where } k'=(6mn+m+3n).\end{aligned}$$

This implies, the product of two integers of the form $(6n+1)$ *and* $(6n+3)$ *is of the form* $(6n+3)$*.*

So the only way for N *to be of the form* $(6n+5)$ *is,* N *must contain at least one factor* r_i *which is of the form* $(6n+5)$*. But* $\nexists$ *any* q_i *of the form* $6n+5$*. If such* q_i *exists, then from construction of* N *we get* $N-6q_1q_2\ldots q_s=-1$*. Furthermore* $N-6q_1q_2\ldots q_s$ *is divisible by a prime of the form* $(6n+5)$*, which contradicts our assumption(Why!).*

3.4 Exercises:

1. Prove each of the assertions below:
   (a) The only prime of the form $n^3-1$is 7.
   (b) The only prime p for which $3p+1$ is a perfect square is $p=5$.
   (c) The only prime of the form n^2-4 is 5.

2. Given that p is a prime and $p\big|a^n$, prove that $p^n\big|a^n$.

3. Establish each of the following statements:
   (a) If $n > 4$ is composite, then n divides $(n-1)!$.
   (b) Any integer of the form $8^n + 1$, where $n \geq 1$, is composite.

4. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.

5. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

6. A positive integer n is called square-full, or powerful, if $p^2\big|n$ for every prime factor p of n (there are 992 square-full numbers less than $250,000$). If n is square-full, show that it can be written in the form $n = a^2b^3$, with a and b positive integers.

7. Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that $n > 1$ is either a prime or the product of two primes.

8. Show that any composite three-digit number must have a prime factor less than or equal to 31.

9. Let q_n be the smallest prime that is strictly greater than $P_n = p_1p_2\ldots p_n+1$. It has been conjectured that the difference $q_n - (p_1p_2\ldots p_n)$ is always prime. Confirm this for the first five values of n.

10. Let p_n denotes the n-th prime number and set $d_n = p_{n+1} - p_n$. Find five solutions of the equation $d_n = d_n + 1$.

11. For $n > 3$, show that the integers $n, n+2, n+4$ cannot all be prime.

12. A conjecture of Lagrange (1775) asserts that every odd integer greater than 5 can be written as a sum $p_l + 2p_2$, where p_1, p_2 are both primes. Confirm this for all odd integers through 75.

13. Show that 13 is the largest prime that can divide two successive integers of the form $n_2 + 3$.

14. Determine all twin primes p and $q = p + 2$ for which $pq - 2$ is also prime.

15. Let p_n denote the n-th prime. For $n > 3$, show that $p_n < p_l+p_2+\ldots+p_{n-l}$.

4

Theory of Congruences

> *"Number theorists are like lotus-eaters—having tasted this food they can never give it up."*
>
> – Leopold Kronecker

4.1 Introduction

If two numbers a and b be such that the difference $a-b$ is divisible by an integer n, then a and b are said to be "Congruent modulo n". The number n is called the modulus and the statement "a is congruent to $b(\bmod n)$" is analytically written as

$$a \equiv b(\bmod n).$$

The quantity a is often said to be the base and the quantity b is called the residue or remainder. There are several types of residues. The common residue defined to be the non-negative and smaller than n while the minimal residue is b or $b-n$, whichever is smaller than absolute terms.

Perhaps, congruence arithmetic is mostly treated as a generalisation of the arithmetic of the clock. Since there are 60 minutes in an hour, "minute arithmetic" uses a modulus of $n=60$. If a person starts at 30 minutes past the hour and then waits for another 55 minutes, $30+55 \equiv 25(\bmod 60)$, so the current time would be 25 minutes past the next hour. By similar way, "hour arithmetic" on a 12 hour clock uses a modulus of $n=12$, so 9 O' clock (a.m) plus four hours give $9+4 \equiv 1(\bmod 12)$ or 1 O' clock (p.m).

Theory of congruences are extremely useful in many areas of number theory. Test of divisibility is one of them.For instance, if the sum of the digits of an integer is divisible by 3, then the original integer is divisible by 3.

Also, congruences have their own restrictions. For instance, knowing the number of minutes past the hour is useful but knowing the hour the minutes are past is often more useful. So congruences discard absolute information. Also, if $a \equiv b(\bmod n)$ and $c \equiv d(\bmod n)$, then it follows that $a^x \equiv b^x(\bmod n)$, but not usually $x^c \equiv x^d(\bmod n)$ or $a^c \equiv b^d(\bmod n)$.

4.2 Congruences

The language of congruences was developed at the beginning of the nineteenth century by famous Mathematician Gauss. The language of congruence is extremely useful in number theory.

Definition 4.2.1. *If a and b are integers, we say that a is congruent to b modulo m if $m|(a-b)$, symbolically denoted by $a \equiv b(\bmod m)$. If a and b are incongruent modulo m, then $m \nmid (a-b)$ and is denoted by $a \not\equiv b(\bmod m)$.*

Example 4.2.1. *Since $6|(20-2) = 18$, therefore, $20 \equiv 2(\bmod 6)$. Similarly, $4 \equiv -5(\bmod 9)$ and $300 \equiv 6(\bmod 7)$.*

In working with congruences, the following proposition is needed.

Proposition 4.2.1. *If a and b are integers, then $a \equiv b(\bmod m)$ if and only if there is an integer l such that $a = b + lm$.*

Proof. Let $a \equiv b(\bmod m)$ hold. Then $m|(a-b)$ implies there exists an integer l such that $a = b+lm$. Conversely, if there exists an integer l such that $a = b+lm$ holds, then $a - b = lm$ implies $l|(a-b)$ implies $a \equiv b(\bmod m)$. $\square$

Here we have given an example to understand the above theorem lucidly.

Example 4.2.2. *Let us consider $16 \equiv 2(\bmod 7)$. Then $16 - 2 = 14$ is divisible by 7 and also we can write 16 as $16 = 2 + 2 \times 7$.*

In the following theorem, we have shown some standard properties related to congruence relation which depicts how an algebraic operations(addition, subtraction, or multiplication) to both sides of a congruence preserves the congruence.

Theorem 4.2.1. *If a, b, c, d and m are integers with $m > 0$ satisfying $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then*

1. $a \pm c \equiv b \pm d(\bmod m)$
2. $ac \equiv bd(\bmod m)$

3. $a \pm c \equiv b \pm c(\bmod m)$

4. $ac \equiv bc(\bmod m)$

5. $a(\bmod m) \equiv b(\bmod m)$.

Proof. 1. Here $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$ implies $m|(a-b)$ and $m|(c-d)$, which further implies there exists integers k and l satisfying $a-b=km$ and $c-d=lm$. From the identity $(a \pm c)-(b \pm d) = (a-b) \pm (c-d) = km \pm lm = m(k \pm l)$, we see both $m|\big((a+c)-(b+d)\big)$ and $m|\big((a-c)-(b-d)\big)$ as $k+l,\ k-l$ both are integers. Therefore $a \pm c \equiv b \pm d(\bmod m)$.

2. Here $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$ implies $m|(a-b)$ and $m|(c-d)$, this again implies that $(c-d)b,\ (a-b)c$ both are divisible by m. Thus, $(a-b)c+(c-d)b = (ac-bd)$ is divisible by m. Therefore $ac \equiv bd(\bmod m)$.

3. Since $a \equiv b(\bmod m)$, therefore $m|(a-b)$. Now $(a \pm c)-(b \pm c) = a-b$ is divisible by m. Therefore $a \pm c \equiv b \pm c(\bmod m)$.

4. Note that $a \equiv b(\bmod m) \Rightarrow m|(a-b)$. Now $(a-b)c = ac-bc$ is divisible by m. Therefore $ac \equiv bc(\bmod m)$.

5. As $a \equiv b(\bmod m)$, then for some integer k we have $a-b=km$. Now k can be written as $k=k_1-k_2$ where k_1, k_2 are integers. Again, $a-b = (k_1-k_2)m = k_1m-k_2m \Rightarrow a-k_1m = b-k_2m = r$. Therefore $r \equiv a(\bmod m)$, $r \equiv b(\bmod m) \Rightarrow a(\bmod m) \equiv b(\bmod m)$.

□

Example 4.2.3. *Since* $18 \equiv 3(\bmod 5)$ *and* $22 \equiv 2(\bmod 5)$, *using Theorem (4.2.1) we see that* $40 = 18+22 \equiv 3+2 \equiv 0(\bmod 5), -4 = 18-22 \equiv 3-2 \equiv 1(\bmod 5)$ *and* $396 = 18 \cdot 22 \equiv 3 \cdot 2 \equiv 6(\bmod 5)$.

Example 4.2.4. *Since* $27 \equiv 3(\bmod 8)$, *it follows* $34 = 27+7 \equiv 3+7 \equiv 10(\bmod 8), 23 = 27-4 \equiv 3-4 \equiv -1(\bmod 8)$, *and* $25 = 27-2 \equiv 3-2 \equiv 1(\bmod 8)$.

Next before proceeding further, the following example reflects the fact that a congruence is not necessarily retained when divided both sides by an integer.

Example 4.2.5. *We have* $20 = 10 \cdot 2 \equiv 4 \cdot 2 = 8(\bmod 6)$. *But* $5 \not\equiv 2(\bmod 6)$.

However, the next theorem provides us with a well-founded congruence when both sides of a congruence are divided by the same integer.

Theorem 4.2.2. *If* a, b, c *and* m *are integers such that* $m > 0, d = \gcd(c, m)$ *and* $ac \equiv bc(\text{mod } m)$*, then* $a \equiv b\big(\text{mod } \dfrac{m}{d}\big)$*.*

Proof. Here $ac \equiv bc(\text{mod } m)$ implies $m|(ac-bc) = c(a-b)$, which further implies there exists an integer k satisfying $c(a-b) = km$. Dividing both sides by d, we have $\dfrac{c}{d}(a-b) = \dfrac{km}{d}$. Since $\gcd\big(\dfrac{c}{d}, \dfrac{m}{d}\big) = 1$, it follows $\dfrac{m}{d}|(a-b) \Rightarrow a \equiv b\big(\text{mod } \dfrac{m}{d}\big)$. □

Theorem(4.2.2) has a corollary that is worth a separate statement.

Corollary 4.2.1. *For any arbitrary positive integers* a *and* b*,* $lcm(a, b) = ab$ *if and only if* $\gcd(a, b) = 1$*.*

Proof. Obvious. □

Example 4.2.6. *Since* $15 = 5(\text{mod } 10)$ *and* $\gcd(5, 10) = 5$*, we see that* $\dfrac{15}{5} \equiv \dfrac{5}{5}\big(\text{mod } \dfrac{10}{5}\big)$ *or* $3 \equiv 1(\text{mod } 2)$*.*

Example 4.2.7. *Since* $42 \equiv 7(\text{mod } 5)$ *and* $\gcd(5, 7) = 1$*, we can conclude that* $\dfrac{42}{7} = \dfrac{7}{7}\big(\text{mod } 5\big)$*, or that* $6 \equiv 1(\text{mod } 5)$*.*

In our next theorem using the principle of mathematical induction we have shown that if we increase the exponential power of elements of both sides of a congruence then the congruence relation is preserved.

Proposition 4.2.2. *Let* a*,* b *be any two integers. For some integer* $m > 0$*, if* $a \equiv b(\text{mod } m)$ *holds then for any positive integer* n*,* $a^n \equiv b^n(\text{mod } m)$ *is also true.*

Proof. We are going to prove this theorem by the principle of mathematical induction. As $a \equiv b(\text{mod } m)$ then the result is obviously true for $n = 1$. Let us assume the result is true for $n = k$. Then $a^k \equiv b^k(\text{mod } m)$ holds. Now using the property(2) of Theorem (4.2.1)we have $a^{k+1} \equiv b^{k+1}(\text{mod } m)$. Thus the result is true for $n = k + 1$. Therefore from the principle of mathematical induction the result is true for all n. □

Example 4.2.8. *Here in this example we have tried to clarify the above proposition by an example. For that let us choose* $8 \equiv 3(\text{mod } 5)$ *then for* $n = 3$ *we see that* $8^3 = 512 \equiv 27 = 3^3(\text{mod } 5)$*.*

In our following theorem we have shown the way to combine congruences of two same numbers with different congruent moduli. To prove this theorem, first we need to prove the following result.

Result 4.2.1. *Let* a *be any integer and* n_1, n_2 *be two positive integers with* $n_1 | a$, $n_2 | a$. *Then* $lcm(n_1, n_2) | a$.

Proof. Let l be the least common multiple of n_1 and n_2. If $l \nmid a$, then the division algorithm yields $m = lq + r$ for some integers q and r where $0 \leq r < l$. Then $r = m - lq$. As l and m are multiples of a and b, then there exists integers $t_1, t_2 t'_1, t'_2$ such that $m = at_1 = bt'_1$, $l = at_2 = bt'_2$. Therefore $r = at_1 - at_2q = a(t_1 - t_2q)$ and $r = bt'_1 - bt'_2q = b(t'_1 - t'_2q)$. This shows that r is a multiple of both a and b. As l is least, then $r \geq l$. This contradicts the fact $0 < r < l$. Therefore $m = lq \Rightarrow l | m$. □

Now the proof of the main theorem as follows.

Theorem 4.2.3. *For any integers* a *and* b *with positive integers* $t_1, t_2, \cdots t_k$ *if* $a \equiv b(\bmod t_1), a \equiv b(\bmod t_2), \cdots, a \equiv b(\bmod t_k)$ *then* $a \equiv b(\bmod lcm(t_1, t_2, \cdots, t_k))$.

Proof. Since $a \equiv b(\bmod t_1), a \equiv b(\bmod t_2), \cdots, a \equiv b(\bmod t_k)$ then we have, $t_1 | (a - b)$, $t_2 | (a - b), \cdots t_k | (a - b)$. Now by above result we can say that $lcm(t_1, t_2, \cdots, t_k) | (a - b)$. This implies $a \equiv b(\bmod lcm(t_1, t_2, \cdots, t_k))$. □

In next corollary, we are going to describe an useful consequence of the above theorem.

Corollary 4.2.2. *For any integers* a *and* b *with positive relatively prime integers* $t_1, t_2, \cdots t_k$ *if* $a \equiv b(\bmod t_1), a \equiv b(\bmod t_2), \cdots, a \equiv b(\bmod t_k)$ *then* $a \equiv b(\bmod (t_1 t_2 \cdots t_k))$.

Proof. Since $a \equiv b(\bmod t_1), a \equiv b(\bmod t_2), \cdots, a \equiv b(\bmod t_k)$, therefore $t_1 | (a - b)$, $t_2 | (a - b), \cdots t_k | (a - b)$. As $t_1, t_2, \cdots t_k$ are relatively prime integers, therefore $lcm(t_1, t_2, \cdots, t_k) = t_1 t_2 \cdots t_k$. Then Theorem 4.2.3 gives $a \equiv b(\bmod (t_1 t_2 \cdots t_k))$. □

In the following proposition we have seen that the congruence relation is nothing but an equivalence relation.

Proposition 4.2.3. *Let* m *be any non-zero integer. Define a relation* ‘$\equiv \bmod m$’ *on set of integers* $\mathbb{Z}$ *by* $a \equiv b(\bmod m)$ *if and only if* $m | (a - b)$. *The relation* ‘$\equiv \bmod m$’ *is an equivalence relation.*

Proof. A relation on a set is said to be equivalence if it is reflexive, symmetric and transitive.

1. Reflexivity: Since $m | (a - a)$, we see that $a \equiv a(\bmod m)$.

2. Symmetricity: If $a \equiv b(\bmod m)$, then $m|(a-b)$. Hence there exists an integer l such that $a-b=lm$. This shows that $(-l)m=b-a \Rightarrow m|(b-a)$. Consequently, $b \equiv a(\bmod m)$.
3. Transitivity: Let $a \equiv b(\bmod m)$ and $b \equiv c(\bmod m)$. Then $m|(a-b)$ and $m|(b-c)$ holds. Hence there exists integers k and l such that $a-b=km$ and $b-c=lm$. Therefore $a-c=(a-b)+(b-c)=km+lm=(k+l)m$. Consequently, $m|(a-c)$ implies $a \equiv c(\bmod m)$.

□

Infact this equivalence relation is also called congruence relation. From the basic concept of algebra we can say that this equivalence relation always forms an equivalence class. In this case this is called congruence class. For example if we choose a positive integer 5 which leaves the remainder $0,1,2,3,4$ when divides any integer. Here if we choose remainder as 1 then we have the set of integers $\{6,11,16,\cdots\}$ whose all the elements have remainder 1 when divided by 5. For that the above set can be written as [1] which is a congruence class modulo 5. Thus the definition of congruence class as follows.

Definition 4.2.2. *Let m be a positive integer and a be any integer then set of integers, $\{b : b \equiv a(\bmod m)\}$ is called congruence class modulo m and denoted by $[a]$.*

From the above definition of congruence class another important fact we can discuss on integers. If we choose a set of integers say, $\{5,21,-2,62,34\}$ then for congruent modulo 5 we have, $5 \equiv 0(\bmod 5)$, $21 \equiv 1(\bmod 5)$, $62 \equiv 2(\bmod 5)$, $-2 \equiv 3(\bmod 5)$, $34 \equiv 4(\bmod 5)$. Here we see that each of the elements of the above set are congruent modulo 5 with exactly one of the set $\{0,1,2,3,4\}$. Then this arbitrary set $\{5,21,-2,62,34\}$ is said to be a complete set of residue modulo 5. Now we are in the position to define that arbitrary set.

Definition 4.2.3. *An arbitrary set of m integers $\{a_1,a_2,\cdots,a_m\}$ is said to be a complete set of residue modulo m or CRS$(\bmod m)$ if every integer of the set is congruent modulo m to exactly one of $a_1,a_2,\cdots,a_m$. More specifically if,*

1. $a_i \not\equiv a_j(\bmod m)$, $\forall i \neq j$, $i,j=1,2,\cdots m$
2. *For each integer n, there exists a unique integer a_j such that* $n \equiv a_j(\bmod m)$, $j=1,2,\cdots m$.

Obviously the set $\{0,1,2,\cdots,m-1\}$ forms a CRS$(\bmod m)$. It is called trivial CRS$(\bmod m)$. For an example if we choose $m=5$ then the set $\{0,1,2,3,4\}$ is the trivial CRS$(\bmod 5)$.

Now in the following theorems we have shown here that addition and multiplication of any arbitrary element with all the elements of a complete residue system under some conditions preserves the properties of complete residue system.

Theorem 4.2.4. *If* $\{a_1, a_2, \cdots, a_m\}$ *is a set of complete residue system modulo* m *and* c *be any integer then* $\{a_1 + c, a_2 + c, \cdots, a_m + c\}$ *is also a set of complete residue system modulo* m*.*

Proof. It's suffices to show that all the elements of $\{a_1 + c, a_2 + c, \cdots, a_m + c\}$ are distinct under congruent modulo m. Since $\{a_1, a_2, \cdots, a_m\}$ is a set of complete residue system modulo m then $a_i \not\equiv a_j$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. Thus $a_i - a_j$ is not divisible by m. Also, $(a_i + c) - (a_j + c) = a_i - a_j$ which follows that $(a_i + c) - (a_j + c)$ is not divisible by m. Therefore $a_i + c \not\equiv a_j + c (\bmod m)$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. This proves the theorem. □

Theorem 4.2.5. *If* $\{a_1, a_2, \cdots, a_m\}$ *is a set of complete residue system modulo* m *and* c *be any integer prime to* m*, then* $\{ca_1, ca_2, \cdots, ca_m\}$ *is also a set of complete residue system modulo* m*.*

Proof. Again here to prove this theorem we are to show all the elements of $\{ca_1, ca_2, \cdots, ca_m\}$ are distinct under congruent modulo m. Since $\{a_1, a_2, \cdots, a_m\}$ is a set of complete residue system modulo m then $a_i \not\equiv a_j$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. Thus $a_i - a_j$ is not divisible by m. Also we have $ca_i - ca_j = c(a_i - a_j)$. Now c is prime to m implies $\gcd(c, m) = 1$ and $a_i - a_j$ is not divisible by m. Combining these two concepts we can conclude that $ca_i - ca_j$ is not divisible by m. Therefore $ca_i \not\equiv ca_j (\bmod m)$ for $i \neq j$ where $i, j = 1, 2, \cdots m$. This proves the assertion of this theorem. □

Combining the above two theorems, lead us to the following straightforward corollary:

Corollary 4.2.3. *If* $\{a_1, a_2, \cdots, a_m\}$ *is a set of complete residue system modulo* m *and* c *be any integer prime to* m*, then* $\{ca_1 + d, ca_2 + d, \cdots, ca_m + d\}$ *is also a set of complete residue system modulo* m *for any integer* d*.*

4.3 Worked out Exercises

Problem 4.3.1. *Give an example to show that* $a^2 = b^2 (\bmod n)$ *need not imply that* $a \equiv b (\bmod n)$*.*

Solution 4.3.1. *Let us consider* $a = 5, b = 4, m = 3$*. Since* $3\big|(25-16) = 9$*, therefore* $5^2 \equiv 4^2 (\bmod 3)$*. But* $5 \not\equiv 4 (\bmod 3)$*.*

Problem 4.3.2. *What is the remainder when the sum* $1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$ *is divided by* 4*?*

Solution 4.3.2. *Here*

$$\begin{aligned} 1^5 &\equiv 1(\bmod 4) & \qquad 1 &\equiv 5 \equiv 9 \ldots (\bmod 4) \\ 32 = 2^5 &\equiv 0(\bmod 4) & 2 &\equiv 6 \equiv 10 \ldots (\bmod 4) \\ 243 = 3^5 &\equiv 3(\bmod 4) & 3 &\equiv 7 \equiv 11 \ldots (\bmod 4) \\ 4^5 &\equiv 0(\bmod 4) & 4 &\equiv 8 \equiv 12 \ldots (\bmod 4). \end{aligned}$$

Each block of four numbers will have same remainder sum. Since $1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 0 + 3 + 0 \equiv 4 \equiv 0(\bmod 4)$*, therefore* 25 *blocks will all have remainder* 0 *implies entire remainder is* 0*.*

Problem 4.3.3. *For* $n \geq 1$*, use congruence theory to establish* $27\big|(25^{n+1} + 5^{n+2})$*.*

Solution 4.3.3. *Here* $32 \equiv 5(\bmod 27) \Rightarrow 2^5 \equiv 5(\bmod 27)$*. Now*

$$\begin{aligned} 2^{5n} &\equiv 5^n (\bmod 27) \\ 2 \cdot 2^{5n} &\equiv 2 \cdot 5^n (\bmod 27). \\ \therefore\; 2^{5n+1} + 2^{5n+2} &\equiv 2 \cdot 5^n + 5^{n+2} (\bmod 27) \\ &\equiv 5^n(5 + 25)(\bmod 27) \\ &\equiv 5^n \cdot 27(\bmod 27) \\ &\equiv 0(\bmod 27). \end{aligned}$$

Problem 4.3.4. *Find the remainder when the sum* $1! + 2! + 3! + \ldots + 100!$ *is divided by* 18*.*

Solution 4.3.4. *Note that* $6! \equiv 0(\bmod 18) \Rightarrow (6+n)! \equiv 0(\bmod 18)$ *for* $n \in \mathbb{Z}$*. Then*

$$\begin{aligned} 1! + 2! + 3! + \cdots + 100! &\equiv (1! + 2! + 3! + 4! + 5!)(\bmod 18) \\ &\equiv 153(\bmod 18) \\ &\equiv 9(\bmod 18). \end{aligned}$$

Therefore the remainder is 9*.*

Problem 4.3.5. *Prove for any integer* a*,* $a^3 \equiv 0, 1,$ *or* $6(\bmod 7)$*.*

Solution 4.3.5. *By division Algorithm, we have* $a = 7k + r,\ 0 \le r < 7$. *Now*

$$a = 7k : a^3 = (7k)^3 = 7 \cdot 7^2k^3 \Rightarrow a^3 \equiv 0(\mod 7).$$
$$a = 7k + 1 : a^3 = (7k+1)^3 = (7k)^3 + 3 \cdot (7k)^2 + 3 \cdot 7k + 1.$$
$$\therefore\ a^3 - 1 = 7[7^2k^3 + 3 \cdot 7k^2 + 3 \cdot k] \Rightarrow a^3 \equiv 1(\mod 7)$$

By similar way, $a = 7k + 2 : a^3 \equiv 1(\mod 7)$

$$a = 7k + 3 : a^3 \equiv 6(\mod 7)$$
$$a = 7k + 4 : a^3 \equiv 1(\mod 7)$$
$$a = 7k + 5 : a^3 \equiv 6(\mod 7)$$
$$a = 7k + 6 : a^3 \equiv 1(\mod 7).$$

Problem 4.3.6. *If* $\{a_1, a_2, \ldots, a_n\}$ *is a complete set of residues modulo* n *and* $\gcd(a, n) = 1$, *prove that* $\{aa_1, aa_2, \ldots, aa_n\}$ *is also a complete set of residues modulo* n.

Solution 4.3.6. *Consider* aa_i *and* aa_j *with* $i \ne j,\ 1 \le i < j \le n$. *If* aa_i *and* aa_j *are congruent moduli* n, *then* $aa_i - aa_j = kn \Rightarrow a(a_i - a_j) = kn$ *for some* k. *Since* $\gcd(a, n) = 1$, *Euclid's Lemma gives* $n \big| (a_i - a_j)$, *contradicting the fact* $a_i \not\equiv a_j$. *Therefore* $aa_i \equiv aa_j$. *Hence by Proposition 4.2.1, the statement follows.*

Problem 4.3.7. *Find the remainder when* 10^{515} *is divided by* 7.

Solution 4.3.7. *Here* $515 = 85 \times 6 + 5 \Rightarrow 10^{515} = (10^6)^{85} \cdot 10^5$. *Further,*

$$\begin{aligned} & 10^2 \equiv 2(\mod 7) \\ \Rightarrow\ & 10^6 \equiv 2^3 \equiv 1(\mod 7) \\ \Rightarrow\ & (10^6)^{85} \equiv 1(\mod 7) \\ \Rightarrow\ & 10^{515}(10^6)^{85} \cdot 10^5 \equiv 1 \cdot 5 \equiv 5(\mod 7). \end{aligned}$$

So the desired remainder is 5.

Problem 4.3.8. *Verify that if* $a \equiv b(\mod n_1)$ *and* $a \equiv b(\mod n_2)$, *then* $a \equiv b(\mod n)$, *where the integer* $n = lcm(n_1, n_2)$. *Hence whenever* n_1 *&* n_2 *are relatively prime,* $a \equiv b(\mod n_1 n_2)$.

Solution 4.3.8. *Let* $k_1, k_2 \in \mathbb{Z}$ *be such that* $a - b = k_1 n_1$, *&* $a - b = k_2 n_2$. *Let* $d = \gcd(n_1, n_2)$. *Then* $\exists\ r \in \mathbb{Z}$ *such that* $n_1 = dr$.

$$\therefore\ a - b = k_2 n_2 = k_2 n_2 \frac{n_1}{dr} = \frac{k_2}{r} \frac{n_1 n_2}{d}.$$

But $\frac{n_1 n_2}{d} = lcm(n_1, n_2)$*[refer to Theorem 2.5.1].*

$$\therefore\ a - b = \frac{k_2}{r} lcm(n_1, n_2).$$

Finally, our aim is to show $\frac{k_2}{r} \in \mathbb{Z}$*. Let* $s \in \mathbb{Z}$ *be such that* $n_2 = ds$*. Since* $a - b = k_1 n_1 = k_2 n_2$*, then* $k_1 dr = k_2 ds \Rightarrow k_1 r = k_2 s$*. Since* $\gcd(r, s) = 1$*, therefore* r *divides* k_2*. This shows that* $\frac{k_2}{r} \in \mathbb{Z}$*.*

Problem 4.3.9. *Show that* 41 *divides* $2^{40} - 1$*.*

Solution 4.3.9. *Here* $2^{20} = (2^5)^4 = (32)^4$*. This shows that* $2^{20} = (32)^4 \equiv (-9)^4 \equiv (81)^2 (\mathrm{mod}\ 41)$*. However* $81 \equiv -1 (\mathrm{mod}\ 41) \Rightarrow 2^{20} \equiv 1 (\mathrm{mod}\ 41)$*. Hence* $41 \big| (2^{20} - 1)$*.*

Problem 4.3.10. *Justify,* $a^k \equiv b^k (\mathrm{mod}\ n)$ *and* $k \equiv j (\mathrm{mod}\ n)$ *need not imply that* $a^j \equiv b^j (\mathrm{mod}\ n)$*.*

Solution 4.3.10. *Since* $4 \equiv 9 (\mathrm{mod}\ 5)$*, therefore*

$$\begin{aligned} 2^2 &\equiv 3^2 (\bmod 5), \\ 2 &\equiv 7 (\bmod 5), \\ 2^7 &\not\equiv 3^7 (\bmod 5) [\textit{Verify!}]. \end{aligned}$$

Problem 4.3.11. *If* $\gcd(a, n) = 1$*, then prove that the integers* $c, c + a, c + 2a, c + 3a, \ldots, c + (n - 1)a$ *form a complete set of residues modulo* n *for any* c*.*

Solution 4.3.11. *Consider* $c + ra$ & $c + sa$, $r \neq s$, $0 \leq r, s \leq n - 1$*. Suppose* $s > r$*.*

$$\therefore\ c + sa - (c + ra) = (s - r)a.$$

Note that $s \leq n - 1$, $r \leq n - 1$ *together implies* $s - r < n$*. Therefore* $n \nmid (s - r)$*. Since* $\gcd(a, n) = 1$*, therefore* $\nexists\ k \in \mathbb{Z}$ *such that* $(s - r)a = nk \Rightarrow c + sa \not\equiv c + ra$*. This completes the solution.*

Problem 4.3.12. *Find all CRS modulo* 6*.*

Solution 4.3.12. *Here the set* $\{0, 1, 2, 3, 4, 5\}$ *forms trivial CRS modulo* 6*. By virtue of Theorem(4.2.4)and Theorem(4.2.5), we conclude that* $\{k, k + a, k + 2a, k + 3a, k + 4a, k + 5a\}$ *forms a CRS modulo* 6*, where* k *is any arbitrary integer and* a *is an integer prime to* 6*.*

Problem 4.3.13. *Prove that the integer* $53^{103} + 103^{53}$ *is divisible by* 39*.*

Solution 4.3.13. *Note that* $39 = 3 \cdot 13,\ 53 = 3 \cdot 17 + 2 = 3 \cdot 18 - 1,\ 103 = 34 \cdot 3 + 1$. *Now*

$$\begin{array}{ll} 53 \equiv -1(\mod 3) & 53 \equiv 1(\mod 13) \\ 53^{103} \equiv (-1)^{103}(\mod 3) & 53^{103} \equiv 1(\mod 13). \end{array}$$

Furthermore,

$$\begin{array}{ll} 103 \equiv 1(\mod 3) & 103 \equiv -1(\mod 13) \\ 103^{53} \equiv 1^{53}(\mod 3) & 103^{53} \equiv -1(\mod 13). \end{array}$$

Adding those congruences with respect to modulo 3 *and modulo* 13 *we get,* $53^{103} + 103^{53} \equiv 0(\bmod 3)$ *and* $53^{103} + 103^{53} \equiv 0(\bmod 13)$ *respectively. This yields* $3\big|(53^{103} + 103^{53}),\ 13\big|(53^{103} + 103^{53})$. *Since* $\gcd(3, 13) = 1$, *therefore* $3 \cdot 13 = 39\big|(53^{103} + 103^{53})$.

4.4 Linear Congruences

The present section deals with the notion of linear equation in the sense of congruence relation. Consider a linear equation of the form $2x + 3y = 5$ with two unknown integers x and y. Then it can be expressed as $y = \dfrac{5 - 2x}{3}$. If we consider $\dfrac{5 - 2x}{3}$ as an integer then the above linear equation can be written as $2x \equiv 5(\bmod y)$. The foregoing congruence relation with unknown integer x is said to be linear congruence equation, whose definition is as follows:

Definition 4.4.1. *A congruence of the form* $ax \equiv b(\bmod m)$ *where* a, b, m *are integers with* $m > 0$ *and* x *an unknown integer, is called linear congruence in one variable.*

Here we have dealt with the various aspects of linear congruences. In the beginning, we have tried to relate linear congruences with the linear Diophantine equation of two variables x and y. Our following theorem is based on that.

Theorem 4.4.1. *Let* (x_0, y_0) *be an integral solution of* $ax + by = c$ *for some integers* a, b, c *where* a, b *are non zero integers then* x_0 *is the solution of* $ax \equiv c(\bmod m)$ *considering* $m = |b|$. *Conversely, if* x_0 *is a solution of the above congruence then there is an integer* y_0 *for which* (x_0, y_0) *is a solution of* $ax + by = c$.

Proof. Since (x_0, y_0) satisfies $ax + by = c$ then we have $by_0 = c - ax_0$. This shows that b divides $ax_0 - c$. Therefore $m = |b|$ divides $ax_0 - c$ and x_0 becomes a solution of $ax \equiv c(\bmod m)$.

For the converse part we have x_0 a solution of $ax \equiv c(\bmod m)$. Since $m = |b|$ divides $ax_0 - c$ then for some integer y_0 we can write $ax_0 - c = by_0$. This proves that (x_0, y_0) satisfies $ax + by = c$. □

Now we are going to illustrate the above fact by following examples.

Example 4.4.1. Here we have shown that a linear Diophantine equation $221x + 35y = 11$ can be solved using linear congruence. Firstly the equation $221x + 35y = 11$ has been written as $221x \equiv 11(\bmod 35)$. Here the solution of this congruence equation is $x \equiv 1(\bmod 35)$. Then we have $x = 1 + 35t$ for some integer t. Here $x_0 = 1$ is the particular value of x and $y_0 = \frac{1}{35}[11 - 221 \cdot 1] = -6$ is particular value of y . Therefore $y = -6 - 221t,\ x = 1 + 35t$ is the general solution.

Example 4.4.2. Let us choose the congruence equation $5x \equiv 2(\bmod 26)$ and this has been written as $5x - 26y = 2$ for some integer y. Here $\gcd(5, 26) = 1$ can be written as $1 = 26 - 5 \cdot 5$. Thus here the particular value of x is $x_0 = -10$. Then we have $x = -10 - 26t$ for some integer t. Therefore $x \equiv -10 \equiv 16($ mod 26) is the solution of above congruence.

Here in the Example 4.4.1 we have solved the linear Diophantine equation by converting it to linear congruence equation and also from the Example 4.4.2 we have solved the linear congruence equation by converting it to linear Diophantine equation. So from the above two examples we can say that the linear congruences and linear diophantine equations are relatable.

In particular, we have seen that $x = x_0$ is a solution of $ax \equiv b(\bmod m)$ then any integer $x_1 \equiv x_0(\bmod m)$ is also a solution. Thus if we can find a particular solution x_0 of $ax \equiv b(\bmod m)$, then all the elements belonging to the class of x_0, are the solutions of $ax \equiv b(\bmod m)$. For instance, choose $4x \equiv ($ mod 5) where $x = 2$ is a solution. Now it's obvious that all the elements of $[2]$ such as $x = 7, 12$ and so on are its solutions. Now the question arises, how many incongruent solutions modulo m do exist?. The following theorem reflects, under which condition it is possible to find a solution of a linear congruence equation and if the solutions exist, how many of them are incongruent modulo m.

Theorem 4.4.2. *Let a, b, m are integers with $m > 0$ then the linear congruence $ax \equiv b(\bmod m)$ has a solution if and only if $d|b$, where $d = \gcd(a, m)$. If $d|b$ then it has exactly d numbers of incongruent solutions.*

Proof. Theorem 4.4.1 asserts that any linear congruence $ax \equiv b(\bmod m)$ is equivalent to linear Diophantine equation $ax - my = b$, for any integer y. So for particular integer x_0 satisfying $ax_0 \equiv b(\bmod m)$ we get an integer y_0 satisfying $ax_0 - my_0 = b$. Again by virtue of Theorem 2.7.1, if $d \nmid b$ then $\nexists$ any solutions. Also, if $d|b$ then the Diophantine equation $ax + mk = b$ have infinite number of solutions given by $x = x_0 + (\frac{m}{d})n$, $k = k_0 - (\frac{a}{d})n$ for some integer n. Here k_0 is a particular value for k. Then comparing both the diophantine equations, yields $y = -k$. Thus, the solutions of $ax - my = b$ are given by

$$x = x_0 + (\frac{m}{d})n,\ -y = -k_0 - (\frac{a}{d})n \Rightarrow y = k_0 + (\frac{a}{d})n.$$

Next, to determine the number of incongruent solutions of $ax \equiv b(\bmod m)$, consider $x_1 = x_0 + (\frac{m}{d})n_1$ and $x_2 = x_0 + (\frac{m}{d})n_2$ as two solutions of $ax \equiv b(\bmod m)$ for some integers n_1, n_2. If these two are congruent then,

$$x_0 + (\frac{m}{d})n_1 \equiv x_0 + (\frac{m}{d})n_2 (\bmod m).$$
$$\therefore (\frac{m}{d})n_1 \equiv (\frac{m}{d})n_2 (\bmod m)$$

Now, $\gcd(m, \frac{m}{d}) = \frac{m}{d}$ and $(\frac{m}{d})|m$. So using Theorem 4.2.2 we obtain $n_1 \equiv n_2(\bmod m)$. This proves that $x = x_0 + (\frac{m}{d})n$ has exactly d numbers of incongruent solutions as n ranges through a complete residue system of residues modulo d. □

In the above theorem, taking a and m as relatively prime integers gives a straightforward corollary:

Corollary 4.4.1. *If a and m are relatively prime then the linear congruence $ax \equiv b(\bmod m)$ has a unique solution modulo m.*

Next our aim is to exemplify the foregoing theorem and corresponding corollary by an example:

Example 4.4.3. *Consider the linear congruence $8x \equiv 16(\bmod 24)$. Since $\gcd(8, 24) = 8$ and $8|16$, using the last theorem our aim is to show that $\exists$ 8 incongruent solutions modulo 24. Here $x_0 = 2$ is a particular solution. Then $x \equiv 2 + (\frac{24}{8})t \equiv 2 + 3t(\bmod 24)$ are the incongruent solutions modulo 24 where $t = 0(1)7$. Thus the solutions are $x \equiv 2, 5, 8, 11, 14, 17, 20, 23(\bmod 24)$. Now, if we choose the congruence $8x \equiv 16(\bmod 23)$ then $\gcd(8, 23) = 1$. Then by virtue of the last corollary, it has only one incongruent solution modulo 23 which is $x \equiv 2(\bmod 23)$.*

Example 4.4.4. *Consider the linear congruence* $8x \equiv 16 \pmod{24}$. *Since* $\gcd(8,24) = 8$ *and* $8|16$, *using the last theorem our aim is to show that* $\exists$, 8 *incongruent solutions modulo* 24. *Here* $x_0 = 2$ *is a particular solution. Then* $x \equiv 2 + (\frac{24}{8})t \equiv 2 + 3t \pmod{24}$ *are the incongruent solutions modulo* 24 *where* $t = 0(1)7$. *Thus the solutions are* $x \equiv 2, 5, 8, 11, 14, 17, 20, 23 \pmod{24}$. *Now, if we choose the congruence* $8x \equiv 16 \pmod{23}$ *then* $\gcd(8,23) = 1$. *Then by virtue of the last corollary, it has only one incongruent solution modulo* 23 *which is* $x \equiv 2 \pmod{23}$.

After solving a linear congruence equation, we are turning our discussion to solve a simultaneous system of linear congruences. This system actually came from Chinese puzzles as early as the first century A.D. In number theory, the Chinese remainder theorem gives a unique solution to simultaneous linear congruences with coprime moduli. In its basic form, the Chinese remainder theorem will determine a number p that, when divided by some given divisors, leaves given remainders.

The earliest known statement of the theorem is by the Chinese mathematician Sun-tzu Suan-ching in the 3rd century AD, whose original formulation was $x \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 2 \pmod 7$ with the solution $x = 23 + 105k$ where $k \in \mathbb{Z}$.

The Chinese remainder theorem is widely used for computing with large integers, as it allows replacing a computation for which one knows a bound on the size of the result by several similar computations on small integers.

Theorem 4.4.3. *(Chinese Remainder Theorem): Let* $m_1, m_2, \cdots m_k$ *be pairwise relatively prime integers. Then for k number of integers* $a_1, a_2, \cdots a_k$ *the system of congruences* $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \cdots x \equiv a_k \pmod{m_k}$ *has a unique solution modulo* $M = m_1 m_2 \cdots m_k$.

Proof. Let $M_r = \frac{M}{m_r} = m_1 m_2 \cdots m_{r-1} m_{r+1} \cdots m_k$ is the product of all integers omitting m_r, shows that $\gcd(M_r, m_r) = 1$. Then from the Corollary 4.4.1 it is possible to find a unique solution x_r of the linear congruence $M_r x \equiv 1 \pmod{m_r}$. Our task is to show that the integer $\tilde{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots a_k M_k x_k$ is a simultaneous solution of the above system. First our aim is to check, $\tilde{x}$ satisfies $x \equiv a_1 \pmod{m_1}$. Since all the integers $M_2, M_3, \cdots M_k$ contain m_1 as a factor so $a_i M_i x_i \equiv 0 \pmod{m_1}$ for all $i = 2, 3, \cdots k$, then $\tilde{x} \equiv a_1 M_1 x_1 \pmod{m_1}$. As $M_1 x_1 \equiv 1 \pmod{m_1}$ it follows that $\tilde{x} \equiv a_1 \pmod{m_1}$. This shows that $\tilde{x}$ satisfies the linear congruence $x \equiv a_1 \pmod{m_1}$. Proceeding as above, we can show that $\tilde{x}$ also satisfies other congruences.

To proceed for the uniqueness part, let x' and $\tilde{x}$ be its two solutions. Then we have $x^{'} \equiv a_r \equiv \tilde{x} (\bmod\ m_r)$ for $r = 1, 2, \cdots, k$. Therefore m_r divides $(x^{'} - \tilde{x})$ for each $r = 1, 2, \cdots, k$. Since all m_r's are relatively prime then from Corollary 2.4.1 we have $M = m_1 m_2 \cdots m_k | (x^{'} - \tilde{x})$. This implies $x^{'} \equiv \tilde{x} (\bmod\ M = m_1 m_2 \cdots m_k)$. Therefore $\tilde{x}$ is the unique solution of the given system. □

In the following example, we have illustrated the preceding theorem lucidly.

Example 4.4.5. *Let us consider a system of simultaneous linear congruences as* $x \equiv 2(\bmod\ 3)$, $x \equiv 4(\bmod\ 5)$, $x \equiv 5(\bmod\ 7)$. *Here* $M = 3 \cdot 5 \cdot 7 = 105$ *then we have* $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$. *As* $M_r x_r \equiv 1(\bmod\ m_r)$ *so the linear congruences are* $35x_1 \equiv 1(\bmod\ 3)$, $21x_2 \equiv 1(\bmod\ 5)$, $15x_3 \equiv 1(\bmod\ 7)$. *Those linear congruences are satisfied by* $x_1 = 2$, $x_2 = 1$, $x_3 = 1$ *respectively. Thus a solution of the system is given by* $\tilde{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 = 140 + 84 + 75 \equiv 299(\bmod\ 105)$. *Thus the unique solution of this system is* $\tilde{x} \equiv 89(\bmod\ 105)$.

4.5 Worked out Exercises

Problem 4.5.1. *Solve:* (1) $36x \equiv 8(\bmod\ 102)$ (2) $140x \equiv 133(\bmod\ 301)$.

Solution 4.5.1. 1. *Since* $\gcd(36, 102) = 6 \nmid 8$, *therefore* $\nexists$ *any solution.*

2. *Here* $140 = 2^2 \cdot 5 \cdot 7$, $301 = 7 \times 43$. *Therefore* $\gcd(140, 301) = 7$ *and* $7 | 133$. *Hence* 7 *incongruent solutions do exist. Dividing both sides of the congruence by* 7 *we have,*

$$\begin{aligned} 20x &\equiv 19(\bmod\ 43) \\ 40x &\equiv 38 \\ 43x - 40x &\equiv 43 - 38(\bmod\ 43) \\ 3x &\equiv 5(\bmod\ 43) \\ 42x &\equiv 70(\bmod\ 43) \\ 43x - 42x &\equiv 86 - 70(\bmod\ 43) \\ x &\equiv 16(\bmod\ 43). \\ \therefore\ x &\equiv 16 + 43t, \ \textit{for}\, t = 0, 1, 2, 3, 4, 5, 6. \\ \therefore\ x &\equiv 16, 59, 102, 145, 188, 231, 274(\bmod\ 301). \end{aligned}$$

Problem 4.5.2. *Using congruences, solve the Diophantine equations:* $12x + 25y = 331$.

Solution 4.5.2. *Note that*

$$\begin{aligned}
12x &\equiv 331(\mod 25),\\
\textit{or, } 24x &\equiv 662(\mod 25),\\
\textit{or, } 25x-24x &\equiv 662-650(\mod 25),\\
\textit{or, } x &\equiv 12(\mod 25).\\
\therefore\; x &= 12+25u,\ \forall u\in\mathbb{Z}.\\
\textit{Further},\ 25y &\equiv 331(\mod 12),\\
\textit{or, } 25y-24y &\equiv 331-324(\mod 12),\\
\textit{or, } y &\equiv 7(\mod 12).\\
\therefore\; y &= 7+12v,\ \forall v\in\mathbb{Z}.\\
\therefore\; 12x+25y &= 12(12+25u)+25(7+12v),\\
\textit{or, } 331 &= 319+300u+300v,\\
\textit{or, } 12 &= 25u+25v.\\
\therefore\; x &= 12+25u = 24-25v.
\end{aligned}$$

Hence $x = 24-25v,\ y = 7+12v$ *for* $v\in\mathbb{Z}$.

Problem 4.5.3. *Solve:* $x\equiv 5(\text{mod } 6),\ x\equiv 4(\text{mod } 11),\ x\equiv 3(\text{mod } 17)$.

Solution 4.5.3. *Here*

$$\begin{aligned}
x &\equiv 5(\mod 6) & N &= 6\cdot 11\cdot 17 = 1122.\\
x &\equiv 4(\mod 11) & N_1 &= 11\cdot 17 = 187.\\
x &\equiv 3(\mod 17) & N_2 &= 6\cdot 17 = 102.\\
 & & N_3 &= 6\cdot 11 = 66.
\end{aligned}$$

Now $187x_1\equiv 1(\text{mod } 6)\Rightarrow 187x_1-186x_1 = x_1\equiv 1(\text{mod } 6)$. *Again*

$$\begin{aligned}
102x_2 &\equiv 1(\mod 11) & 66x_3 &\equiv 1(\mod 17)\\
102x_2-99x_2 = 3x_2 &\equiv 1(\mod 11) & 66x_3-68x_3 = -2x_3 &\equiv 1(\mod 17)\\
21x_2 &\equiv 7(\mod 11) & 18x_3 &\equiv -9(\mod 17)\\
21x_2-22x_2 = -x_2 &\equiv 7(\mod 11) & 18x_3-17x_3 = x_3 &\equiv -9(\mod 17).
\end{aligned}$$

$$\therefore\; x_1 = 1,\ x_2 = -7,\ x_3 = -9.$$

$$\therefore\; a_1N_1x_1 = 5\cdot 187\cdot 1,\ a_2N_2x_2 = 4\cdot(102)\cdot(-7),\ a_3N_3x_3 = 3\cdot(66)\cdot(-9).$$

$$\therefore\; a_1N_1x_1+a_2N_2x_2+a_3N_3x_3 = -3703.$$

$$\therefore\; x\equiv -3703+4\cdot 1122 = 785(\mod 1122).$$

Problem 4.5.4. *Obtain three consecutive integers, each having a square factor.*

Solution 4.5.4. *Note that* $a \equiv 0(\bmod 2^2)$, $a+1 \equiv 0(\bmod 3^2)$, $a+2 \equiv 0(\bmod 5^2)$. *Since* $2^2, 3^2$ *and* 5^5 *are relatively prime to each other, therefore by virtue of Chinese Remainder Theorem we find*

$$\begin{aligned} a &\equiv 0(\bmod 4) & N &= 4\cdot 9\cdot 25 = 900\\ a &\equiv -1(\bmod 9) & N_1 &= 9\cdot 25 = 225\\ a &\equiv -2(\bmod 25) & N_2 &= 4\cdot 25 = 100\\ & & N_3 &= 4\cdot 9 = 36. \end{aligned}$$

Now $225x_1 \equiv 1(\bmod 4) \Rightarrow 225x_1 - 224x_1 = x_1 \equiv 1(\bmod 4)$. *Again*

$$\begin{aligned} 100x_2 &\equiv 1(\bmod 9) & 36x_3 &\equiv 1(\bmod 25)\\ 100x_2 - 99x_2 &\equiv 1(\bmod 9) & 72x_3 &\equiv 2(\bmod 25)\\ x_2 &\equiv 1(\bmod 9) & 72x_3 - 75x_3 &\equiv -3(\bmod 25)\\ & & 3x_3 &\equiv -2(\bmod 25)\\ & & 24x_3 &\equiv -16(\bmod 25)\\ & & 24x_3 - 25x_3 = -x_3 &\equiv -16(\bmod 25)\\ & & x_3 &\equiv 16(\bmod 25). \end{aligned}$$

$$\therefore\ a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = -1252.$$

$$\therefore\ x \equiv 548(\bmod 900).$$

Thus the desired three consecutive numbers are 548, 549, 550.

Problem 4.5.5. *Prove that the congruences* $x \equiv a(\bmod n)$ *and* $x \equiv b(\bmod m)$ *admit a simultaneous solution if and only if* $\gcd(n,m)\big|(a-b)$; *if a solution exists, confirm that it is unique modulo* $lcm(n,m)$.

Solution 4.5.5. *Suppose there exists a solution for* x. *Let* $d = \gcd(n,m)$. *This implies* $\exists\, r,s \in \mathbb{Z}$ *such that* $n = dr, m = ds$. *Now*

$$\begin{aligned} x &\equiv a(\bmod n) \Rightarrow x = a + nt, t \in \mathbb{Z},\\ x &\equiv b(\bmod m) \Rightarrow x = b + mk, k \in \mathbb{Z}. \end{aligned}$$

$$\therefore\ a + nt = b + mk \Rightarrow nt - mk = b - a.$$

Substituting for m, n *we obtain*

$$d(sk - rt) = a - b \Rightarrow d = \gcd(n,m)\big|(a-b).$$

Next, let us assume $d = \gcd(m, n)$ *and* $d|(a-b)$. *Then for some* $t \in \mathbb{Z}, dt = a - b \Rightarrow \exists\ x_0, y_0$ *such that* $nx_0 + my_0 = d$. *Therefore* $dt = nx_0t + my_0t = a - b \Rightarrow my_0t + b = a - x_0tn$. *Let* $x \equiv a(\text{mod } n)$, $x \equiv b(\text{mod } m)$. *So* $\exists$ *a simultaneous solutions. Let* y *be any other solution. Then*

$$\begin{aligned} & x \equiv a(\mod n) && y \equiv a(\mod n). \\ & x \equiv b(\mod m) && y \equiv b(\mod m). \\ \therefore\ & x \equiv y(\mod n). \\ & x \equiv y(\mod m). \end{aligned}$$

By virtue of worked out Problem 4.3.8, we obtain $x \equiv y(\text{mod } lcm(m, n))$.

Problem 4.5.6. *A certain integer between* 1 *and* 1200 *leaves the remainders* 1, 2, 6 *when divided by* 9, 11, 13, *respectively. What is the integer?*

Solution 4.5.6. *From the given conditions, we have*

$$\begin{aligned} & x \equiv 1(\mod 9), && 1 < x < 1200. \\ & x \equiv 2(\mod 11), \\ & x \equiv 6(\mod 13). \end{aligned}$$

Since 9, 13, 11 *are relatively prime, therefore Chinese Remainder Theorem is applicable here. Rest proceeding similarly as in Problem 4.5.4, we obtain the integer* 838.

Problem 4.5.7. *Obtain the two incongruent solutions modulo* 210 *of the system:*

$$\begin{aligned} 2x &\equiv 3(\mod 5) \\ 4x &\equiv 2(\mod 6) \\ 3x &\equiv 2(\mod 7). \end{aligned}$$

Solution 4.5.7. *Here*

$$2x \equiv 3(\mod 5) \tag{4.5.1}$$
$$4x \equiv 2(\mod 6) \tag{4.5.2}$$
$$3x \equiv 2(\mod 7). \tag{4.5.3}$$

$$\begin{aligned} \textit{From}(4.5.1),\ 4x &\equiv 6(\mod 5), & \textit{From}(4.5.2),\ 4\frac{x}{2} &\equiv \frac{2}{2}(\mod \frac{6}{2}), \\ 4x - 5x = x &\equiv 1(\mod 5), & 2x &\equiv 1(\mod 3), \\ x &\equiv -1 + 5(\mod 5), & 4x &\equiv 2(\mod 3), \\ x &\equiv 4(\mod 5). & 4x - 3x = x &\equiv 2(\mod 3), \\ & & x &\equiv 2(\mod 6). \end{aligned}$$

Since $\gcd(4,6) = 2$*, therefore from Theorem 4.4.2 we can say that there* $\exists\ 2$ *incongruent solutions given by* $x_0, x_0 + \frac{6}{2}, x_0$ *being a solution. Here* $x_0 = 2$ *is a solution, so* 5 *is the other. Therefore* $x \equiv 5 \pmod 6$ *is the other congruence equation. From (4.5.3), we obtain*

$$\begin{aligned}
6x &\equiv 4(\bmod 7),\\
6x - 7x = -x &\equiv -3(\bmod 7),\\
-x &\equiv -3(\bmod 7),\\
\therefore\ x &\equiv 3(\bmod 7).
\end{aligned}$$

Therefore $x \equiv 4 \pmod 5$, $x \equiv 2 \pmod 6$ *or* $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod 7$. *Note that* $N = 5 \cdot 6 \cdot 7 = 210$. *Therefore* $N_1 = 6 \cdot 7 = 42$, $N_2 = 5 \cdot 7 = 35$ *and* $N_3 = 5 \cdot 6 = 30$. *Thus*

$$\begin{aligned}
42x_1 &\equiv 1(\bmod 5)\\
42x_1 - 40x_1 = 2x_1 &\equiv 1(\bmod 5).\\
6x_1 &\equiv 3(\bmod 5)\\
6x_1 - 5x_1 = x_1 &\equiv 3(\bmod 5)\\
x_1 &\equiv 3(\bmod 5).\\
30x_3 &\equiv 1(\bmod 7)\\
30x_3 - 28x_3 = 2x_3 &\equiv 1(\bmod 7)\\
8x_3 &\equiv 4(\bmod 7)\\
8x_3 - 7x_3 = x_3 &\equiv 4(\bmod 7).
\end{aligned}$$

$$\begin{aligned}
35x_2 &\equiv 1(\bmod 6)\\
35x_2 - 36x_2 = -x_2 &\equiv 1(\bmod 6)\\
x_2 &\equiv 5(\bmod 6).
\end{aligned}$$

Therefore $a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = 1214$ *or* 1739*(Verify!). Thus the solutions are* $x \equiv 164 \pmod{210}$ *or* $x \equiv 59 \pmod{210}$.

Problem 4.5.8. *Obtain the eight incongruent solutions of the linear congruence* $3x + 4y \equiv 5 \pmod 8$.

Solution 4.5.8. *Set* $3x \equiv 5 - 4y \pmod 8$. *Since* $\gcd(3,8) = 1$ *and* $1|(5-4y)$, *there exists one solution for any value of* y. *Because there are eight incongruent values of* $5 - 4y(y = 0,1,2,3,4,5,6,7)$, *let us solve this for each values of* y. *First, let us take* $y \equiv 0 \pmod 7$. *Then*

$$\begin{aligned}
3x &\equiv 5(\bmod 8)\\
15x &\equiv 25(\bmod 8)\\
16x - 15x = x &\equiv -1 \equiv 7(\bmod 8).
\end{aligned}$$

By similar reasoning, $x \equiv 3(\mod 8)$ *for* $y \equiv 1(\mod 8)$*,* $x \equiv 7(\mod 8)$ *for* $y \equiv 2(\mod 8)$*,* $x \equiv 3(\mod 8)$ *for* $y \equiv 3(\mod 8)$*,* $x \equiv 7(\mod 8)$ *for* $y \equiv 4(\mod 8)$*,* $x \equiv 3(\mod 8)$ *for* $y \equiv 5(\mod 8)$*,* $x \equiv 7(\mod 8)$ *for* $y \equiv 6(\mod 8)$ *and* $x \equiv 3(\mod 8)$ *for* $y \equiv 7(\mod 8)$*.*

Problem 4.5.9. *The basket-of-eggs problem is often phrased in the following form: One egg remains when the eggs are removed from the basket* 2, 3, 4, 5*, or* 6 *at a time; but, no eggs remain if they are removed* 7 *at a time. Find the smallest number of eggs that could have been in the basket.*

Solution 4.5.9. *From the given conditions, we have*

$$x \equiv 1(\mod 2) \tag{4.5.4}$$

$$x \equiv 1(\mod 3) \tag{4.5.5}$$

$$x \equiv 1(\mod 4) \tag{4.5.6}$$

$$x \equiv 1(\mod 5) \tag{4.5.7}$$

$$x \equiv 1(\mod 6) \tag{4.5.8}$$

$$x \equiv 0(\mod 7). \tag{4.5.9}$$

If (4.5.6) is true, then $x = 1 + 4n = 1 + 2(2n)$*. Since* $\gcd(2, 4) \neq 1$*, therefore we can eliminate (4.5.4). Moreover, if (4.5.8) is true, then* $x = 1 + 6n = 1 + 3(2n)$*. Because* $\gcd(3, 6) \neq 1$*, whence we can eliminate (4.5.5). Multiplying (4.5.6) by* 3 *and (4.5.8) by* 2*, we obtain*

$$3x \equiv 3(\mod 3 \cdot 4) = 3(\mod 12) \tag{4.5.10}$$

$$2x \equiv 2(\mod 2 \cdot 6) = 2(\mod 12). \tag{4.5.11}$$

$$\therefore\ 3x - 3 \equiv 2x - 2(\mod 12),$$

$$x \equiv 1(\mod 12). \tag{4.5.12}$$

If (4.5.12) holds true, then (4.5.6) and (4.5.8) is also so. Now we have $x \equiv 1(\mod 5)$*,* $x \equiv 0(\mod 7)$ *and* $x \equiv 1(\mod 12)$*. Note that* 5, 7, 12 *are relatively prime. Thus* $N = 5 \cdot 7 \cdot 12 = 420$*. Therefore* $N_1 = 7 \cdot 12 = 84$*,* $N_2 = 5 \cdot 12 = 60$ *and* $N_3 = 5 \cdot 7 = 35$*. Hence*

$$\begin{aligned} 84x_1 &\equiv 1(\mod 5) & 35x_3 &\equiv 1(\mod 12) \\ 84x_1 - 85x_1 = -1x_1 &\equiv 1(\mod 5) & 35x_3 - 36x_3 = -x_3 &\equiv 1(\mod 12) \\ x_1 &\equiv -1(\mod 5). & x_3 &\equiv 5 - 1(\mod 12). \end{aligned}$$

Since $a_2 = 0$*, therefore* $60x_2 \equiv 1(\mod 7)$*. Thus* $a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 = -119$*(Verify!). Hence* $-119 + 420 = 301$ *eggs in basket.*

4.6 System of Linear Congruences

In this section, our discussion will be restricted to solve the system of linear congruence equations involving the same numbers of unknowns with the same modulus.

Let us begin with an example. Consider the system of linear congruence equations:

$$x + 2y \equiv 1 (\bmod 5) \tag{4.6.1}$$

$$2x + y \equiv 1 (\bmod 5). \tag{4.6.2}$$

Now (4.6.1) × 2 − (4.6.2) yields

$$3y \equiv 1 (\bmod 5).$$

Note that 2 is the inverse of 3 modulo 5. So multiplying both sides of the foregoing equation by 2 we get,

$$y \equiv 2 (\bmod 5).$$

Similarly, (4.6.2) × 2 − (4.6.1) we get,

$$3x \equiv 1 (\bmod 5).$$

Since 2 is the inverse of 3 modulo 5, therefore proceeding as above we get

$$x \equiv 2 (\bmod 5).$$

Thus the solutions of the system of linear congruences are in pairs satisfying $x \equiv 2 (\bmod 5)$ and $y \equiv 2 (\bmod 5)$.

This example motivates us to devise a general method for solving the system of linear congruences.

Theorem 4.6.1. *Let p, q, r, s, u, v and m be integers with $m > 0$, such that $\gcd(D, m) = 1$ where $D = ps - qr$. Then the system of congruences*

$$px + qy \equiv u (\bmod m) \tag{4.6.3}$$

$$rx + sy \equiv v (\bmod m) \tag{4.6.4}$$

has a unique solution modulo m given by,

$$x \equiv \bar{D}(us - qv) (\bmod m)$$

$$y \equiv \bar{D}(pv - ur) (\bmod m)$$

where $\bar{D}$ is the inverse of D modulo m.

Proof. Let us begin with a calculation. Here (4.6.3) $\times\, s$ – (4.6.4) $\times\, q$ yields

$$Dx \equiv (us - qv) (\text{mod } m).$$

Since $\bar{D}$ is the inverse of D modulo m, therefore multiplying both sides by $\bar{D}$ we get

$$x \equiv \bar{D}(us - qv) (\text{mod } m).$$

Similarly, applying $\bar{D}$ on (4.6.3) $\times\, r$ – (4.6.4) $\times\, s$ gives

$$y \equiv \bar{D}(pv - ur) (\text{mod } m).$$

Our claim is that any pair (x, y) is a solution. For this we have,

$$\begin{aligned} px + qy &\equiv \bar{D}\{p(us - qv) + q(pv - ur)\} (\text{mod } m) \\ &\equiv \bar{D}u(ps - qr) (\text{mod } m) \\ &\equiv \bar{D}Du (\text{mod } m) \\ &\equiv u(\text{ mod } m) \\ \text{and } rx + sy &\equiv \bar{D}\{r(us - qv) + s(pv - ur)\} (\text{mod } m) \\ &\equiv \bar{D}v(ps - qr) (\text{mod } m) \\ &\equiv \bar{D}Dv (\text{mod } m) \\ &\equiv v (\text{mod } m). \end{aligned}$$

This proves the theorem. □

In the Theorem 4.6.1 we have discussed the solution for a system of two linear congruences with two unknowns. But the method fails for n linear congruences with n unknowns where $n > 2$. To overcome this, we require the algebra of matrices. The following definition on congruence relation between matrices will pave the way for our future discussions.

Definition 4.6.1. *For any two matrices* $S = (s_{ij})_{n\times k}$ *and* $T = (t_{ij})_{n\times k}$, S *is said to be congruent to* T *modulo* $m(> 0)$ *if* $s_{ij} \equiv t_{ij} (\text{mod } m)$ *for every* i *and* j *with* $1 \le i \le n$, $1 \le j \le k$. *This is denoted as* $S \equiv T (\text{mod } m)$.

Example 4.6.1. *Consider* $S = \begin{pmatrix} 8 & 4 \\ 9 & 7 \end{pmatrix}$ *and* $T = \begin{pmatrix} 13 & 4 \\ 14 & 12 \end{pmatrix}$. *Then* $S \equiv T($mod 5).

Proposition 4.6.1. *For any two matrices* $[S]_{n\times k}$ *and* $[T]_{n\times k}$ *with* $S \equiv T (\text{mod } m)$, $\exists$ *matrices* $[U]_{k\times p}$ *and* $[V]_{p\times n}$ *respectively, with all integer entries, such that* $SU \equiv TU (\text{mod } m)$ *and* $VS \equiv VT (\text{mod } m)$.

Proof. Let $S = (s_{ij})_{n\times k}$, $T = (t_{ij})_{n\times k}$ and $U = (u_{ij})_{k\times p}$ be the matrices with integral entries. Now the entries of SU and TU are $\sum_{r=1}^{n} s_{ir}u_{rj}$ and $\sum_{r=1}^{n} t_{ir}u_{rj}$ respectively. Since $S \equiv T \pmod{m}$, therefore we have $s_{ir} \equiv t_{ir} \pmod{m}$ for all i and r. In view of Theorem 4.2.1 we get,

$$\sum_{r=1}^{n} s_{ir}u_{rj} \equiv \sum_{r=1}^{n} t_{ir}u_{rj} \pmod{m}.$$

This proves $SU \equiv TU \pmod{m}$. Similarly we can show that $VS \equiv VT \pmod{m}$. □

We continue our development of the method for solving system of congruences,

$$\begin{aligned} s_{11}x_1 + s_{12}x_2 + \ldots s_{1n}x_n &\equiv t_1 \pmod{m} \\ s_{21}x_1 + s_{22}x_2 + \ldots s_{2n}x_n &\equiv t_2 \pmod{m} \\ &\vdots\vdots \\ s_{n1}x_1 + s_{n2}x_2 + \ldots s_{nn}x_n &\equiv t_n \pmod{m}. \end{aligned}$$

The system can be written as $SX \equiv T \pmod{m}$, where

$$S = \begin{pmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m,1} & s_{m,2} & \cdots & s_{m,n} \end{pmatrix} X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \text{ and } T = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix}.$$

This method is based on finding the inverse $\bar{S}$ of S modulo m. Here $\bar{S}$ is defined as $\bar{S}S \equiv S\bar{S} \equiv I \pmod{m}$, where $I_{n\times n}$ is the identity matrix.

To illustrate this, let us choose $S = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Then $\bar{S} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$ where $S\bar{S} = \begin{pmatrix} 11 & 5 \\ 25 & 11 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}$ and $\bar{S}S = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{5}$. Next proposition describes a method for finding inverses of 2×2 matrices.

Proposition 4.6.2. *Let* $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be a matrix with integer entries and* m *be a positive integer such that* $D = \det S = ad - bc$ *with* $\gcd(D, m) = 1$*. Then the matrix* $\bar{S} = \bar{D}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ *is the inverse of* S *modulo* m*, where* $\bar{D}$ *is the inverse of* D *modulo* m*.*

Proof. Whether $\bar{S}$ is the inverse of S, it suffices to examine $S\bar{S} \equiv \bar{S}S \equiv I(\bmod m)$. For this, let us consider

$$S\bar{S} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bar{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \equiv \bar{D} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \equiv \bar{D}D \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv I(\bmod m)$$

$$\bar{S}S \equiv \bar{D} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \bar{D} \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \equiv \bar{D}D \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv I(\bmod m).$$

Since $\bar{D}$ is inverse of D modulo m, therefore $\bar{D}D \equiv 1(\bmod m)$ holds in both the cases. Thus $\bar{S}$ is the inverse of S modulo m. ☐

Finally we are going to conclude with a need to find the solution for the system of congruences $SX \equiv T(\bmod m)$ where S is a $n \times n$ matrix. For that we need to find $\bar{S}$, the inverse of S modulo m. In our last proposition, we have found the inverse $\bar{S}$ for 2×2 matrices. But for $n \times n$ matrices where $n > 2$, we need to find $\bar{S}$ with the notion of the adjoint of a matrix S denoted by *adj* S. Our first task is to find $\bar{S}$ for an $n \times n$ matrix. The following proposition serves this purpose.

Proposition 4.6.3. *Let S be an $n \times n$ matrix with integer entries and m be a positive integer with $\gcd(D, m) = 1$. Then the matrix $\bar{S} = \bar{D}(adj\ S)$ is the inverse of S modulo m where $D = \det S$ and $\bar{D}$ is the inverse of D modulo m.*

Proof. Note that $\gcd(D, m) = 1$ implies $\det S \neq 0$. Now from the property of adjoint of a square matrix, we have

$$S(adj\ S) = (\det S)I = DI.$$

Also $\gcd(D, m) = 1$ implies that $\exists$ an inverse $\bar{D}$ of D modulo m. This follows that,

$$\begin{aligned} &S(\bar{D}(\text{adj}S)) \equiv S(\text{adj}S)\bar{D} \equiv D\bar{D} \equiv I(\bmod m) \text{ and} \\ &\bar{D}(\text{adj}S)S \equiv \bar{D}D \equiv I(\bmod m). \end{aligned}$$

Combining we get $\bar{S} = \bar{D}(\text{adj } S)$ is an inverse of S modulo m. ☐

This leads us to solve the system $SX \equiv T(\bmod m)$. Here if we multiply both sides of the congruence by $\bar{S}$ we obtain,

$$\begin{aligned} \bar{S}(SX) &\equiv \bar{S}T(\bmod m) \\ (\bar{S}S)X &\equiv \bar{S}T(\bmod m) \\ X &\equiv \bar{S}T(\bmod m). \end{aligned}$$

The following example illustrates the fact lucidly.

Example 4.6.2. *Let us consider the system,*

$$\begin{aligned} x+2y+3z &\equiv 1(\text{mod } 7)\\ x+3y+5z &\equiv 1(\text{mod } 7)\\ x+4y+6z &\equiv 1(\text{mod } 7). \end{aligned}$$

This can be written as $SX \equiv T(\text{mod } m)$ *where*

$$S=\begin{pmatrix}1&2&3\\1&3&5\\1&4&6\end{pmatrix},\ X=\begin{pmatrix}x\\y\\z\end{pmatrix}\ \text{and } T=\begin{pmatrix}1\\1\\1\end{pmatrix}.$$

Here $D=\det S=-1$. *Then* $\bar{D}=6$. *Also adj* $S=\begin{pmatrix}-2&0&1\\-1&3&-2\\1&-2&1\end{pmatrix}$. *Thus we have*

$$\bar{S}=6\begin{pmatrix}-2&0&1\\-1&3&-2\\1&-2&1\end{pmatrix}=\begin{pmatrix}-12&0&6\\-6&18&-12\\6&-12&6\end{pmatrix}$$

$$X\equiv\begin{pmatrix}-12&0&6\\-6&18&-12\\6&-12&6\end{pmatrix}\begin{pmatrix}1\\1\\1\end{pmatrix}(\text{mod } 7)\equiv\begin{pmatrix}-6\\0\\0\end{pmatrix}(\text{mod } 7).$$

$\therefore$ *The solution is* $x\equiv 1(\text{mod } 7),\ y\equiv 0(\text{mod } 7),\ z\equiv 0(\text{mod } 7)$.

4.7 Worked out Exercises

Problem 4.7.1. *Find the solution of the system of linear congruences*

$$\begin{aligned} 2x+3y &\equiv 5(\text{mod } 7)\\ x+5y &\equiv 6(\text{mod } 7). \end{aligned}$$

Solution 4.7.1. *Multiplying second equation by* 2 *and then subtracting with first one we get*

$$-7y\equiv -7(\text{ mod } 7).$$

This shows that y *can take any residue modulo* 7. *If* $y=0$, *then* $x\equiv 6(\text{mod } 7)$. *So the first solution is* $(6,0)$. *Continuing this manner we can find other solutions too.*

Problem 4.7.2. *Find the inverse modulo* 5 *for the matrix*

$$S = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$$

Solution 4.7.2. *Here* $D = 4 - 2 = 2$. *Then* $\bar{D}D \equiv 1(\mathrm{mod}\ 5) \Rightarrow \bar{D} = 3$. *Let* $\bar{S}$ *be the inverse of* S. *Then*

$$\bar{S} = 3\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & -6 \\ -3 & 6 \end{pmatrix}. \quad \therefore\ \bar{S} \equiv \begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix} (\ \mathrm{mod}\ 5).$$

Problem 4.7.3. *Find the inverse modulo* 5 *for the matrix*

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{pmatrix}$$

Solution 4.7.3. *Here* $D = 1(12-20) - 2(6-5) + 3(4-2) = -4$. *Then* $\bar{D}D \equiv 1(\ \mathrm{mod}\ 7) \Rightarrow \bar{D} = 5$. *Now*

$$adj\ S = \begin{pmatrix} -1 & 0 & 4 \\ -1 & 3 & -2 \\ 2 & -2 & 0 \end{pmatrix} \textit{ shows } \bar{S} = 5\begin{pmatrix} -1 & 0 & 4 \\ -1 & 3 & -2 \\ 2 & -2 & 0 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{pmatrix} (\ \mathrm{mod}\ 7).$$

4.8 Exercises:

1. Find the remainders when 2^{50} and 41^{65} are divided by 7.

2. Establish the following divisibility statements by theory of congruence for integers $n(\geq 1)$:
   (a) $7 \big| 5^{2n} + 3 \cdot 2^{5n-2}$;
   (b) $17 \big| 2^{3n+1} + 3 \cdot 5^{2n+1}$;
   (c) $43 \big| 6^{n+2} + 7^{2n+1}$.

3. For $n(\geq 1)$, show that $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1}(\mathrm{mod}\ 181)$.

4. Find the remainder when 2^{340} is divided by 341.

5. Prove the assertions below:
   (a)If a is an odd integer, then $a^2 \equiv 1(\mathrm{mod}\ 8)$.
   (b)For any integer a, $a^4 \equiv 0$ or $1(\mathrm{mod}\ 5)$.

6. Prove the following statements:
   (a) The product of any set of n consecutive integers is divisible by n. (b) Any n consecutive integers form a complete set of residues modulo n.

7. Using theory of congruence show that $89 | 2^{44} - 1$ and $97 | 2^{48} - 1$.

8. Solve the following linear congruences:
   (a) $5x \equiv 2 \pmod{26}$;
   (b) $34x \equiv 60 \pmod{98}$.

9. Using congruences, solve the Diophantine equations below:
   (a) $4x + 51y = 9$;
   (b) $5x - 53y = 17$.

10. Solve each of the following sets of simultaneous congruences:
    (a) $x \equiv 5 \pmod{11}, x \equiv 14 \pmod{29}, x \equiv 15 \pmod{31}$;
    (b) $2x \equiv 1 \pmod{5}, 3x \equiv 9 \pmod{6}, 4x \equiv 1 \pmod{7}, 5x \equiv 9 \pmod{11}$.

11. Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

12. Check that whether the system $x \equiv 5 \pmod{6}$ and $x \equiv 7 \pmod{15}$ has a solution or not.

13. Solve the system of congruences,
    $3x + 4y \equiv 5 \pmod{13}$
    $2x + 5y \equiv 7 \pmod{13}$.

14. Find an integer having the remainders $2, 3, 4, 5$ when divided by $3, 4, 5, 6$ respectively.

15. Verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ form a complete set of residues modulo 11, but
    $0, 1, 2^2, 3^2, \ldots, 10^2$ does not.

16. Find the solution of the following system of linear congruences,

$$4x + y \equiv 5 (\mod 7)$$
$$x + 2y \equiv 4 (\mod 7)$$

17. Find the solution of the following system of linear congruences,

$$x + 3y \equiv 1 (\mod 5)$$
$$3x + 4y \equiv 2 (\mod 5).$$

18. Find the inverse modulo 5 for the matrix,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

19. Find the inverse modulo 7 for the matrix,

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

20. Find all solutions of the following system,

$$\begin{aligned} x + y &\equiv 1(\mod 7) \\ x + z &\equiv 1(\mod 7) \\ y + z &\equiv 1(\mod 7). \end{aligned}$$

5

Fermat's Little Theorem

> *"Perhaps, posterity will thank me for having shown that the ancients did not know anything."*
>
> – Pierre De Fermat

5.1 Introduction

The famous French Mathematician Pierre de Fermat first wrote what would become his "Little Theorem" in 1640. It states that for any prime number p and any integer a the expression $(a^p - a)$ is divisible by p as long as p does not divide a(the pair are relatively prime). Although a number n that does not divide $a^n - a$ for some a must be a composite number but the converse is not necessarily true. An example, in the later section of the chapter, will justify the above argument. Thus, Fermat's theorem gives a test that is necessary but not sufficient for primality. Also the theorem is applicable in public-key cryptography.

As was typical of Fermat, no proof by him is known to exist. Although a proof in an unpublished manuscript dated around 1683 was given by German mathematician Gottfried Wilhelm Leibniz but in 1736 the proof, by Swiss Mathematician Leonhard Euler, had been known to be published. Some $2,000$ years old a special case of Fermat's theorem known as the Chinese hypothesis which replaces a with 2, states that a number n is prime if and only if it divides $2^n - 2$. As proved later in the West, the Chinese hypothesis is only half right. Fermat's little theorem concerns modular arithmetic.

5.2 Fermat's Little Theorem

Theorem 5.2.1. *Fermat's Little Theorem: Let p be a prime and $p \nmid a$ then, $a^{p-1} \equiv 1 (\bmod p)$.*

Proof. Let us begin with the first $p-1$ positive multiples of a which are

$$a, 2a, 3a, \cdots, (p-1)a.$$

None of them are congruent modulo p to any other. Then $ra \equiv sa (\bmod p)$ with $1 \leq r < s \leq p-1$ implies $r \equiv s (\bmod p)$, which is not possible. Multiplying we get,

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)(\bmod p) \Rightarrow a^{p-1} \equiv 1(\bmod p).$$

□

This is not the only way to prove the theorem. There are a lot more other interesting ways to prove this theorem. Mathematical induction is one among them. To begin with, we fix a prime p. For this prime p it is obvious that $1^p \equiv 1(\bmod p)$ *i.e.* $1^{p-1} \equiv 1(\bmod p)$, when $a = 1$. Suppose the statement prevails for $a = k$. Then $k^{p-1} \equiv 1(\bmod p)$. Now we have to prove $(k+1)^{p-1} \equiv 1(\bmod p)$ for some base $k+1 \in \mathbb{Z}$ and $p \nmid (k+1)$. Taking aid of binomial theorem we have,

$$(k+1)^p = k^p + \binom{p}{1} k^{p-1} + \cdots + \binom{p}{l-1} k + 1.$$

Because $\binom{p}{l} = \frac{p!}{l!(p-l)!}$ for $1 \leq l \leq p-1$, it follows that p divides every coefficients of the terms of right hand side of the foregoing equation except k^p and 1. Now taking modulo p we have $(k+1)^p \equiv k^p + 1(\bmod p)$. So by induction hypothesis we get $(k+1)^p \equiv k+1(\bmod p)$. Therefore the result holds for $k+1$. Hence the principle of mathematical induction yields $a^p \equiv a(\bmod p)$ *i.e.*$a^{p-1} \equiv 1(\bmod p)$ for all $a \in \mathbb{Z}$ such that $p \nmid a$.

The above two proofs of Fermat's Little theorem are mostly theoretic. Instead, we can provide some experimental ways by means of combinatorics to make the theorem more lively and natural. Choose $p = 3, a = 2$ where $3 \nmid 2$. Consider the following diagrams,

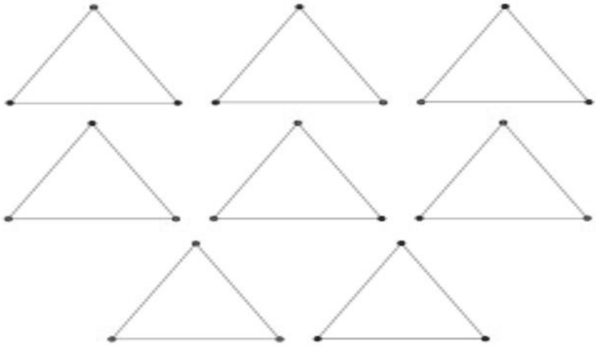


Figure 5.1: Fermat's Little Theorem

Here every angle of the triangles are associated with red and blue coloured balls. There are $2^3 = 8$ ways to pick the colour of the balls. Also we see that $2^3 - 2 = 6$ is divisible by 3. Therefore $2^3 \equiv 2(\bmod 3)$. Thus in general $a^{p-1} \equiv 1(\bmod p)$ holds, where $p \nmid a$.

Our next corollary investigates the question: Can we drop the condition $\gcd(a, p) = 1$?

Corollary 5.2.1. *If p is prime, then $a^p \equiv a(\bmod p)$ for any integer a.*

Proof. When $p \mid a$ then $a^p \equiv 0 \equiv a(\bmod p)$ and if $p \nmid a$ then by above theorem $a^{p-1} \equiv 1(\bmod p)$ implies $a^p \equiv a(\bmod p)$. □

A simple but interesting question to ask: if $a^n \equiv a(\bmod n)$ holds, then does it imply n is prime? The answer is in a negative sense. For instance, pick out $n = 117$. Then taking $a = 2$ we see that $2^{117} = (2^7)^{16} \cdot 2^5$ where $2^7 = 128 \equiv 11(\bmod 117)$. Thus we find $2^{117} \equiv 11^{16} \cdot 2^5(\bmod 117) \equiv 4^8 \cdot 2^5(\bmod 117) \equiv 2^{21}(\bmod 117)$. But $2^{21} = (2^7)^3$. Hence $2^{21} \equiv 11^3(\bmod 117) \equiv 121 \cdot 11(\bmod 117) \equiv 4 \cdot 11(\bmod 117) \equiv 44(\bmod 117) \not\equiv 2(\bmod 117)$. Here we note $117 = 13 \cdot 9$. Hence, if $a^n \equiv a(\bmod n)$ holds then n must be composite.

Our future discussions will be based on some instances where those types of composite numbers even satisfy this congruence relation under some special circumstances.

Lemma 5.2.1. *If p and q are distinct primes with $a^p \equiv a(\bmod q)$ and $a^q \equiv a(\bmod p)$ then, $a^{pq} \equiv a(\bmod pq)$.*

Proof. It is very clear that $(a^p)^q \equiv a^q(\bmod p) \equiv a(\bmod p)$ and $(a^q)^p \equiv a^p(\bmod q) \equiv a(\bmod q)$. So we have $p|a^{pq}$ and $q|a^{pq}$. As $\gcd(p,q) = 1$ then we can directly say that $pq|a^{pq}$. Since $\gcd(a,b) = 1$ and $a|c, b|c$ together imply $ab|c$, therefore $a^{pq} \equiv a(\bmod pq)$. □

So the above lemma highlights the fact that the converse of Fermat's theorem satisfies for some special type of composite numbers which can be expressed as the product of two distinct primes. These types of numbers are said to be pseudo-prime to the base a. Now we are in a position to define pseudoprime viz

Definition 5.2.1. *A composite integer n for which $a^n \equiv a(\bmod n)$ is called a pseudoprime to the base a.*

If $a = 2$ then, it is called pseudo prime to the base 2 or simply pseudoprime.

Let us take $341 = 11 \cdot 31$. So by Fermat's Little Theorem we have $2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1024(\bmod 31) \equiv 2 \cdot 1(\bmod 31) \equiv 2(\bmod 31)$ and $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3(\bmod 11) \equiv 2(\bmod 11)$. Furthermore, $\gcd(11, 31) = 1$. In view of Lemma(5.2.1) we can say that $2^{11 \cdot 31} = 2^{341} \equiv 2(\bmod 341)$ which further yields 341 as a pseudoprime. In fact, the first five pseudoprimes are $341, 561, 645, 1105, 161038$ and the first four are odd. Finding pseudoprimes are difficult as those are rarer than primes. There are only 245 pseudoprimes and 78498 primes less than 10^6. We now try to construct an increasing sequence of pseudoprimes from the following theorem.

Theorem 5.2.2. *There are infinitely many psuedo-primes to the base 2.*

Proof. Let n be a composite number. Then $\exists\ r, s \in \mathbb{Z}$ such that $n = rs$ where $1 < r \leq s < n$. Let $K_n = 2^n - 1$ be any integer where $(2^r - 1)|(2^n - 1)$[refer to Problem(2.6.4)] or $(2^r - 1)|K_n$, making K_n a composite quantity.

As n is pseudo-prime then $2^n \equiv 2(\bmod n)$. Hence $2^n - 2 = kn$ for some $k \in \mathbb{Z}$. Therefore

$$\begin{aligned} 2^{K_n - 1} = 2^{kn} - 1 &= (2^n - 1)[2^{n(k-1)} + \cdots + 2^n + 1] \\ &= K_n[2^{n(k-1)} + \cdots + 2^n + 1] \\ &\equiv 0(\bmod K_n). \end{aligned}$$

Hence $2^{K_n} \equiv 2(\bmod K_n)$. Therefore K_n is a pseudoprime. □

Remark 5.2.1. *The number* $K_n = 2^n - 1$ *shown in the above theorem is said to be Mersenne number, which is named after Father Marin Mersenne* $(1588 - 1648)$*[for further studies refer to Chapter 10 Section 10.4 of this book].*

The above discussion generates the fact that the pseudoprimes are the special type of composite numbers which satisfies the conditions of Fermat's Little theorem. But in pseudoprime, we have a barrier of base element a *i.e.* for these types of numbers the condition of Fermat's theorem does not satisfy for all base elements a. If we consider $561(= 3 \times 11 \times 17)$ with $\gcd(a, 561) = 1$ for any $a \in \mathbb{Z}^+$, we have $\gcd(a, 3) = 1 = \gcd(a, 11) = \gcd(a, 17)$. By virtue of Fermat's theorem, we get $a^2 \equiv 1(\text{mod } 3), a^{10} \equiv 1(\text{mod } 11), a^{16} \equiv 1(\text{mod } 17)$ which imply

$$\begin{aligned} a^{560} &= (a^2)^{280} \equiv 1(\text{ mod } 3) \\ a^{560} &= (a^{10})^{56} \equiv 1(\text{ mod } 11) \\ a^{560} &= (a^{16})^{35} \equiv 1(\text{ mod } 17). \end{aligned}$$

Since $3, 11, 17$ are primes, the last three congruences together conclude $a^{560} \equiv 1(\text{mod } 561)$. Therefore $a^{561} \equiv a(\text{mod } 561)$ for all $a \in \mathbb{Z}^+$ with $\gcd(a, 561) = 1$.

The last example spotlights the fact that 561 is a special type of composite number which satisfies the condition of Fermat's theorem for any integer. R.D.Carmichael first noticed the existence of these types of numbers in the year 1910. Those numbers are called Carmichael numbers named after American Mathematician Carmichael. There are six Carmichael numbers $561, 1105, 1729, 2465, 2821, 6601$ less than $10,000$. There are just 43 Carmichael numbers less than 10^6 and 1547 less than 10^{10}. Thus we are in a position to define the Carmichael number.

Definition 5.2.2. *The composite numbers n which satisfy the property* $a^n \equiv a(\text{mod } n)$ *for all integers a are said to be absolute pseudoprime or Carmichael numbers.*

Next our aim is to establish the criterion for the existence of Carmichael numbers.

Theorem 5.2.3 (Korselt's Criterion)**.** *Let n be a composite square free integers;* $n = p_1 p_2 \cdots p_n$ *where p_i are distinct primes. If* $(p_i - 1)\big|(n-1)$ *for* $i = 1, 2, \cdots, r$ *then n is Carmichael number.*

Proof. Suppose that a is an integer satisfying $\gcd(a, p_i) = 1$ for each i. Then, by Fermat's theorem we have $p_i|(a^{p_i - 1} - 1)$. As $(p_i - 1)|(n-1)$ so $p_i|(a^{n-1} - 1)$, as $p_i|(a^n - a)$, for all a and $i = 1, 2, 3, \cdots, r$. This implies $n\big|(a^n - a)$ for all a. Therefore n is Carmichael number. □

The next theorem supplies the pertinent information about the prime factorizations of Carmichael numbers.

Theorem 5.2.4. *A Carmichael number must have at least three different odd prime factors.*

Proof. Let n be a Carmichael number. Since n is composite and is the product of distinct primes so, it cannot have just one prime factor. Then assume, $n = pq$ for some odd primes p, q with $p > q$. So

$$n - 1 = pq - 1 = (p-1)q + (q-1) \equiv (q-1) \not\equiv 0(\mod p-1),$$

which render $(p-1) \nmid (n-1)$. Since it has just two different prime factors hence, n cannot be a Carmichael number. $\square$

The development of primality of testing can be done further with the following:

Definition 5.2.3. *Let n be a positive integer with $n-1 = 2^k t$ where k is a non–negative integer and t is an odd positive integer. We can say n passes Miller's test for the base a if either $a^t \equiv 1(\mathrm{mod}\ n)$ or $a^{2^i t} \equiv -1(\mathrm{mod}\ n)$ for some i with $0 \leq i \leq k-1$.*

The next theorem shows the idea of primality testing by means of Miller's test.

Theorem 5.2.5. *If n is prime and a is a positive integer with $n \nmid a$, then n passes Miller's test for the base a.*

Proof. Let $n - 1 = 2^k t$ where k is non–negative integer and t is an odd positive integer. Let $z_\omega = a^{\frac{(n-1)}{2^\omega}} = a^{2^{k-\omega}\cdot t}$ for $\omega = 0, 1, 2, \ldots, k$. Since n is prime, by Fermat's little theorem we have $z_0 = a^{n-1} \equiv 1(\mathrm{mod}\ n)$. Furthermore $z_1^2 = \left(a^{\frac{n-1}{2}}\right)^2 = a^{n-1} = z_0 \equiv 1(\mathrm{mod}\ n)$ implies either $z_1 \equiv -1(\mathrm{mod}\ n)$ or $z_1 \equiv 1(\mathrm{mod}\ n)$. If $z_1 \equiv 1(\mathrm{mod}\ n)$ then $z_2^2 = \left(a^{\frac{n-1}{2^2}}\right)^2 = a^{\frac{n-1}{2}} = z_1 \equiv 1(\mathrm{mod}\ n)$. Thus either $z_2 \equiv 1(\mathrm{mod}\ n)$ or $z_2 \equiv -1(\mathrm{mod}\ n)$. Proceeding as above, $z_0 \equiv z_1 \equiv z_2 \cdots z_\omega \equiv 1(\mathrm{mod}\ n)$ for $\omega < k$. Also, $z_{\omega+1}^2 = z_\omega \equiv 1(\mathrm{mod}\ n)$ or $z_{\omega+1} \equiv 1(\mathrm{mod}\ n)$. Thus continuing for $\omega = 1, 2, 3, \ldots, k$ we find that either $z_k \equiv 1(\mathrm{mod}\ n)$ or $z_\omega \equiv -1(\mathrm{mod}\ n)$ for some integer ω with $0 \leq \omega \leq (k-1)$. Hence n passes Miller's test for the base a. $\square$

Let us illustrate the above theorem by the following example. Choose $n = 25 = 5 \cdot 5$. Then $7^{24} = (7^4)^6 \equiv 1(\mathrm{mod}\ 5)$ such that 25 is a pseudoprime to the base 7. Also $24 = 2^3 \cdot 3$ then $7^{2^1 \cdot 3} \equiv -1 (\bmod 25)$. Therefore 25 passes Miller's test for base 7 as well as it is a pseudoprime. So getting motivated from the example we are going to define:

Definition 5.2.4. *If n is composite and passes Miller's test to the base a, then n is called strong pseudoprime to the base a.*

Let us illustrate the ideas behind the definition(5.2.4) with an example of strong pseudoprime which has passed Miller's test. Consider $n = 25326001$. Then $n-1 = 2^4 \times 1582875$. Here we can check that $2^{1582875} \equiv -1 (\bmod 25326001)$. This shows that 25326001 is a strong pseudoprime as it passes Miller's test.

Strong pseudoprimes are rare but there are still infinitely many of them. We conclude this section with a theorem that reflects the existence of an infinite number of strong pseudoprimes to the base 2.

Theorem 5.2.6. *There are infinitely many strong pseudoprimes to the base* 2*.*

Proof. To begin with, suppose n to be an odd pseudoprime base 2. We claim that the composite number $N = 2^n - 1$ is a strong pseudoprime to the base 2. Referring to Problem 2.6.4 we see that if n is composite then $2^n - 1$ is also so. Furthermore, if n is pseudoprime then we have $2^{n-1} \equiv 1 (\bmod n)$. This implies that $2^{n-1} - 1 = nk$ for some odd integer $k (> 0)$. We note that

$$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2nk.$$

As $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 (\bmod N)$ then we can write $2^{\frac{(N-1)}{2}} = 2^{nk} \equiv 1 (\bmod N)$. The argument shows that N passes Miller's test for base 2. Thus N becomes a strong pseudoprime base 2. An appeal to Theorem 5.2.2 concludes that there are infinitely many strong pseudoprime to the base 2. This finishes the proof. □

5.3 Worked out Exercises

Problem 5.3.1. *If* $\gcd(a, 35) = 1$*, show that* $a^{12} \equiv 1 (\bmod 35)$*.*

Solution 5.3.1. *As* $\gcd(a, 35) = 1$*, therefore* $\gcd(a, 7) = 1 = \gcd(a, 5)$*. An appeal to Fermat's theorem indicates* $a^6 \equiv 1 (\bmod 7) \Rightarrow a^{12} = (a^6) \cdot (a^6) \equiv 1 (\bmod 7)$ *and* $a^4 \equiv 1 (\bmod 5) \Rightarrow (a^4)^3 \equiv 1 (\bmod 5)$*. Since* $\gcd(5, 7) = 1$*, it follows that* $35 \big| (a^{12} - 1)$*. Therefore* $a^{12} \equiv 1 (\bmod 35)$*.*

Problem 5.3.2. *If* $\gcd(a, 42) = 1$ *then* $168 = 3 \cdot 7 \cdot 8$ *divides* $a^6 - 1$*.*

Solution 5.3.2. *Because* $\gcd(a,42) = 1$, *therefore* $\gcd(a,7) = \gcd(a,3) = \gcd(a,2) = 1$. *By virtue of Fermat's theorem, we find* $a^6 \equiv 1(\bmod 7)$, $a^2 \equiv 1(\bmod 3)$ *and* $a \equiv 1(\bmod 2)$. *Therefore* $a^6 = (a^2)^3 \equiv 1(\bmod 3)$. *Moreover,* $a^6 - 1 = (a^3-1)(a^3+1) = (a-1)(a+1)(a^2+a+1)(a^2-a+1)$. *Because* a *is odd therefore,* $a > 0 \Rightarrow a \geq 3$. *This yields* $2\big|(a-1)$, $4\big|(a+1)$. *Since* $7, 3, 8$ *are relatively prime to each other, therefore we get* $168\big|(a^6-1)$. *Hence* $8\big|(a^6-1)$.

Problem 5.3.3. *If* $\gcd(a,133) = \gcd(b,133) = 1$ *then, show that* $133|(a^{18}-b^{18})$.

Solution 5.3.3. *We know that* $133 = 7 \cdot 19$ *and* $\gcd(a,19) = \gcd(b,19) = 1$. *Therefore in view of Fermat's theorem we obtain* $a^{18} \equiv 1(\bmod 19)$ *and* $b^{18} \equiv 1(\bmod 19)$. *Hence* $a^{18} - b^{18} \equiv (1-1)(\bmod 19) \equiv 0(\bmod 19)$. *Hence* $19|(a^{18}-b^{18})$. *By similar reasoning,* $7|(a^6-b^6)$. *Since* $a^{18}-b^{18} = (a^6-b^6)\big((a^6)^2 + a^6b^6 + (b^6)^2\big)$, *therefore we have* $7|(a^{18}-b^{18})$. *Thus* $7{\cdot}19 = 133|(a^{18}-b^{18})$.

Problem 5.3.4. *Derive the following congruences:*
(a) $a^{21} \equiv a(\bmod 15)$, $\forall a$. *(b)* $a^7 \equiv a(\bmod 42)$ $\forall a$. *(c)* $a^9 \equiv a(\bmod 30)$ $\forall a$.

Solution 5.3.4. (a) *Taking into consideration the corollary of Fermat's theorem, we find* $a^{21} \equiv a(\bmod 5) \Rightarrow (a^5)^4 \equiv a^4(\bmod 5) \Rightarrow a^{21} \equiv a^5 \equiv a(\bmod 15)$. *Furthermore,* $a^3 \equiv a(\bmod 3) \Rightarrow a^{21} \equiv a^7(\bmod 3)$. *Again,* $(a^3)^2 \equiv a^2(\bmod 3) \Rightarrow a^7 \equiv a^3(\bmod 3) \equiv a(\bmod 3)$. *Hence* $a^{21} \equiv a(\bmod 3)$. *Thus,* $a^{21} \equiv a(\bmod 15)$.

(b) *As* $42 = 7 \cdot 3 \cdot 2$ *by Fermat's theorem we have* $a^7 \equiv a(\bmod 7)$ *and* $a^3 \equiv a(\bmod 3)$. *Therefore* $a^6 \equiv a^2(\bmod 3) \Rightarrow a^7 \equiv a^3(\bmod 3) \equiv a(\bmod 3)$. *Also,* $a^2 \equiv a(\bmod 2) \Rightarrow a^6 \equiv a^3(\bmod 2) \equiv a(\bmod 2) \Rightarrow a^7 \equiv a^2(\bmod 2) \equiv a(\bmod 2)$. *Since* $7, 3, 2$ *are prime to each other therefore,* $a^7 \equiv a(\bmod (7 \cdot 3 \cdot 2)) \Rightarrow a^7 \equiv a(\bmod 42)$.

(c) *Left to the reader.*

Problem 5.3.5. *If* $\gcd(a,30) = 1$, *show that* $60\big|(a^4+59)$.

Solution 5.3.5. *Note that* $\gcd(a,30) = 1$ *implies* $\gcd(a,2) = \gcd(a,3) = \gcd(a,5) = 1$. *So* $\gcd(a,4) = \gcd(a,2^2) = 1$. *Now* $60 = 2^2 \cdot 3 \cdot 5$ *and* $60|(a^4+59)$ *together implies* $a^4 \equiv 1(\bmod 60)$. *Here* $a^2 \equiv 1(\bmod 3)$ *implies* $a^4 \equiv 1(\bmod 3)$ *and* $a^4 \equiv 1(\bmod 5)$. *Further,* $a \equiv 1(\bmod 2) \Rightarrow a^2 \equiv 1(\bmod 2)$ *which leads to* $2\big|(a^2-1)$. *Hence*

$$\begin{aligned} a^2 &\equiv (1-2)(\bmod 2) \\ &\equiv -1(\bmod 2). \end{aligned}$$

Thus, combining the foregoing equation with $2\big|(a^2+1)$ *yields* $2\big|(a^4-1)$. *Since* $3, 4, 5$ *relatively prime to each other, therefore we can conclude* $60|(a^4-1)$. *Hence*

$$\begin{aligned} a^4 &\equiv 1(\mod 60) \\ &\equiv (1-60)(\mod 60) \\ &\equiv -59(\mod 60). \end{aligned}$$

This completes the solution.

Problem 5.3.6. *(a) Find the unit digit of* 3^{100} *using Fermat's theorem.*
(b) For any integer verify that a^5 *and* a *have same unit digit.*

Solution 5.3.6. *(a) Its suffices to consider modulo 10. Now we plan to use Fermat's theorem to get* $3^4 \equiv 1(\mod 5)$. *Therefore* $3^{100} \equiv 1(\mod 5)$. *Moreover* $3 \equiv 1(\mod 2)$. *Hence* $3^{100} \equiv 1(\mod 2)$. *Further* $\gcd(2,5) = 1 \Rightarrow 10\big|3^{100} \equiv 1(\mod 10)$. *Hence the unit digit is* 1.

(b) By virtue of Fermat's theorem, $a^5 \equiv a(\mod 5)$ *and* $a^2 \equiv a(\mod 2)$. *Hence* $a^4 \equiv a^2(\mod 2) \equiv a(\mod 2)$ *implies* $a^5 \equiv a^2(\mod 2) \equiv a(\mod 2)$. *Thus* $a^5 \equiv a(\mod 10)$. *Let* $0 \leq r < 10$ *holds. Then* $a^5 - r \equiv a - r(\mod 10)$. *Therefore* $a^5 - r \equiv 0(\mod 10) \iff a - r \equiv 0(\mod 10)$. *Therefore unit digit's are same.*

Problem 5.3.7. *If* $7 \nmid a$, *then prove that either* $7|(a^3+1)$ *or* $7|(a^3-1)$.

Solution 5.3.7. *By Fermat's theorem,* $a^6 \equiv 1(\mod 7)$. *Therefore* $7|(a^6-1)$ *but* $a^6 - 1 = (a^3-1)(a^3+1)$. *Therefore* $7 \nmid (a^3+1)$ *implies* $7|(a^3-1)$ *and vice–versa.*

Problem 5.3.8. *If* p, q *are distinct odd primes such that* $(p-1)|(q-1)$ *and* $\gcd(a, pq) = 1$, *show that* $a^{q-1} \equiv 1(\mod pq)$.

Solution 5.3.8. *Here* $\gcd(a, pq) = 1$ *implies* $\gcd(a, p) = 1 = \gcd(a, q)$. *Therefore with the help of Fermat's Theorem we get* $a^{p-1} \equiv 1(\mod p)$ *and* $a^{q-1} \equiv 1(\mod q)$. *Since* $(p-1)\big|(q-1)$, *therefore* $q - 1 = k(p-1)(k \in \mathbb{Z})$. *Hence* $(a^{p-1})^k \equiv 1^k(\mod p) \equiv 1(\mod p) \Rightarrow a^{q-1} \equiv 1(\mod p)$. *Thus* $pq|(a^{q-1}-1) \Rightarrow a^{q-1} \equiv 1(\mod pq)$.

Problem 5.3.9. *If* p, q *are distinct primes then prove that* $p^{q-1} + p^{q-1} \equiv 1(\mod pq)$.

Solution 5.3.9. *By virtue of Fermat's theorem,* $p^{q-1} \equiv 1(\mod q)$ *implies* $q^{p-1} \equiv 0(\mod q)$. *Therefore* $p^{q-1} + p^{q-1} \equiv 1(\mod q)$. *Similarly,* $q^{p-1} + p^{q-1} \equiv 1(\mod p)$. *Further,* $\gcd(p, q) = 1$ *yields* $p^{q-1} + p^{q-1} \equiv 1(\mod pq)$.

Problem 5.3.10. *Establish the statement: If* p *is an odd prime, then* $1^{p-1} + 2^{p-1} \cdots (p-1)^{p-1} \equiv (p-1) \equiv -1(\mod p)$.

Solution 5.3.10. *Since p is odd prime, so $p \geq 3$ and $p \nmid a$. if $a < p$ then by Fermat's theorem we have, $a^{p-1} \equiv 1 (\bmod\ p)$. For $p-1$ terms we have,*

1. $1^{p-1} \equiv 1(\bmod\ p)$
2. $2^{p-1} \equiv 1(\bmod\ p)$

$$\vdots$$

3. $(p-1)^{p-1} \equiv 1(\bmod\ p)$.

Therefore $1^{p-1} + 2^{p-1} \cdots (p-1)^{p-1} \equiv (p-1) \equiv -1(\bmod\ p)$.

Problem 5.3.11. *Confirm* $1105 = 5 \cdot 13 \cdot 17$ *is absolute pseudoprime.*

Solution 5.3.11. *For any integer a, if* $1105 \nmid a$ *then* $5 \nmid a$, $13 \nmid a$ & $17 \nmid a$. *So by Fermat's theorem, we have* $a^4 \equiv 1(\bmod\ 5) \Rightarrow a^{1104} = (a^4)^{276} \equiv 1(\bmod\ 5)$. *Also* $a^{12} \equiv 1(\bmod\ 13) \Rightarrow a^{1104} = (a^{12})^{92} \equiv 1(\bmod\ 13)$. *Moreover,* $a^{16} \equiv 1(\bmod\ 17) \Rightarrow a^{1104} = (a^{16})^{69} \equiv 1(\bmod\ 17)$. *As* $5, 13, 17$ *are relatively prime to each other, therefore* $a^{1104} \equiv 1(\bmod\ 1105)$. *Thus* $a^{1105} \equiv a(\bmod\ 1105)$ *provided* $1105 \nmid a$. *Clearly,* $a^{1105} \equiv a(\bmod\ 1105)$ *prevails provided* $1105 \mid a$. *Hence* 1105 *is an absolute pseudo prime as it satisfies* $a^{1105} \equiv a(\bmod\ 1105)$ *for any integer a.*

Problem 5.3.12. *Prove that any integer of the form* $n = (6k+1)(12k+1)(18k+1)$ *is an absolute pseudoprime if all three factors are prime; hence* $1729 = 7 \cdot 13 \cdot 19$ *is also absolute pseudo–prime.*

Solution 5.3.12. *Let* $p_1 = 6k+1, p_2 = 12k+1, p_3 = 18k+1$, *be all primes. Now* $n = 36 \cdot 36k^3 + 36 \cdot 2k^2 + 36 \cdot 9k^2 + 36k + 1$. *Therefore* $n-1 = 36k[36 \cdot k^2 + 11k + 1]$ *gives* $p_1 - 1 \big| n-1, p_2 - 1 \big| n-1$ *and* $p_3 - 1 \big| n-1$. *Since* p_1, p_2, p_3 *are distinct primes and n is square free, therefore n is absolute pseudoprime.*

Problem 5.3.13. *Show that* 561 *is the only Carmichael number of the form* $3pq$ *where p and q are primes.*

Solution 5.3.13. *Let* $n = 3pq$, *with $q > p$ odd primes, be a carmichael number. Then using Korselt's criterion, we obtain* $(p-1) \big| (3pq-1) = 3(p-1)q + 3q - 1$. *So* $(p-1) \big| (3q-1) \Rightarrow (p-1)a = 3q - 1$ *for some* $a \in \mathbb{Z}$. *Since $q > p$, we must have $a \geq 4$. Similarly,* $\exists\ b \in \mathbb{Z}$ *satisfying* $(q-1)a = 3p - 1$. *Solving these two equations for p, q yields*

$$p = \frac{2b + ab - 3}{ab - 9} = 1 + \frac{2b+6}{ab-9}, \tag{5.3.1}$$

$$q = \frac{2a + ab - 3}{ab - 9}. \tag{5.3.2}$$

Since $p > 3$ being odd prime, therefore $4(ab-9) \leq 2b+6$ reduces to $b(2a-1) \leq 21$. Now $a \geq 4 \Rightarrow b \leq 3$. Then,

$$4(ab-9) \leq 2b+6 \leq 12 \Rightarrow ab \leq \frac{21}{4} \Rightarrow a \leq 5.$$

Hence $a = 4$ or 5. If $b = 3$, then the denominator of (5.3.2) is multiple of 3. So the numerator must be multiple of 3, which is impossible as there $\nexists$ any 'a' divisible by 3. Thus $b = 1$ or 2.The denominator of equation (5.3.2) must be positive, so $ab > 9$. Thus the only possible values for a and b is 5 and 2 respectively, which gives $p = 11, q = 17$. So $561 = 3 \cdot 11 \cdot 17$ is the only Carmichael number of the form $3pq$, where p and q are primes.

Problem 5.3.14. *Show that there are only a finite number of Carmichael numbers of the form $n = pqr$ where p is a fixed prime, and q and r are also primes.*

Solution 5.3.14. *Assume $r > q$. Applying Korselt's Criterion, we get $(q-1)\big|(pqr-1) = (q-1)pr + pr - 1$. Therefore $(q-1)\big|(pr-1) \Rightarrow pr - 1 = a(q-1)$ for some $a \in \mathbb{Z}$. Similarly, $pq - 1 = b(r-1)$ for some $b \in \mathbb{Z}$. Since, $r > q$ so $a > b$. Solving last two equations for q and r yields*

$$\begin{aligned} r &= \frac{p(a-1)+a(b-1)}{ab-p^2}, \\ q &= \frac{p(b-1)+b(a-1)}{ab-p^2}. \end{aligned}$$

Because this last fraction must be an integer, we have

$$ab - p^2 \leq p^2 + pb - p - b,$$

which further reduces to

$$\begin{aligned} a(b-1) &\leq 2p^2 + p(b-1), \\ \Rightarrow a - 1 &\leq \frac{2p^2}{b} + \frac{p(b-1)}{b} \leq 2p^2 + p. \end{aligned}$$

So $\exists$ only finite values for a. Likewise, the same inequality gives

$$\begin{aligned} b(a-1) &\leq 2p^2 + p(b-1), \\ \Rightarrow b(a-1-p) &\leq 2p^2 - p. \end{aligned}$$

Since $a > b$ and the denominator of the expression for q must be positive, we have $a \geq p+1$. Now, $a = p+1$ gives

$$(p+1)(q-1) = pq - p + q - 1 = pr - 1 \Rightarrow p|q, \text{ a contradiction.}$$

Therefore $a > p+1 \Rightarrow a-p-1 > 0$. *The last inequality gives us*

$$b \leq b(a-p-1) \leq 2p^2 - p,$$

which shows $\exists$ *finitely many values of* b. *Because* a, b *determine* q, r *respectively, therefore there are only a finite number of Carmichael numbers of the form* $n = pqr$.

Problem 5.3.15. *Show that* 2047 *is a strong pseudoprime base* 2.

Solution 5.3.15. *Here* $n = 2047$ *yields* $n - 1 = 2046 = 2 \times 1023$. *Now* $2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1(\text{mod } 2047)$. *So* 2047 *passes Miller's test for base* 2. *Thus* 2047 *is a strong pseudoprime base* 2.

5.4 Wilson's Theorem

Wilson's theorem, in number theory, signifies that any prime p divides $(p-1)!+1$, where $n!$ is the factorial notation for $1\times2\times3\times4\times\cdots\times n$. For example, 7 divides $(7-1)!+1 = 6!+1 = 721$. The conjecture was first published by the English mathematician Edward Waring in Meditationes Algebraicae (1770 'Thoughts on Algebra'), where he described it to the English mathematician John Wilson.

After that it was proved by the French mathematician Joseph-Louis Lagrange in 1771. The converse of the theorem is also true; that is, $(n-1)!+1$ is not divisible by a composite number n. In theory, these theorems provide a test for primes; in practice, the calculations are impractical for large numbers.

Theorem 5.4.1. *Wilson's Theorem: If p is a prime then* $(p-1)! \equiv -1(\text{mod } p)$.

Proof. Let us choose $p > 3$ and consider the linear congruence $ax \equiv 1(\text{mod } p)$ where a is any one of $1, 2, 3, \cdots, p-1$. Therefore $\gcd(a, p) = 1$. Hence, it has an unique solution viz $a\tilde{a} \equiv (\text{mod } p)$ with $1 \leq \tilde{a} \leq p-1$. Because p is prime, $a = \tilde{a} \Leftrightarrow a = 1$ or $a = p-1$ provided $a^2 \equiv 1(\text{mod } p) \Rightarrow (a-1)(a+1) \equiv 0(\text{mod } p)$. Therefore $(a-1) \equiv 0(\text{mod } p)$ or $(a+1) \equiv 0(\text{mod } p)$. Now if we delete 1 and $p-1$, then the remaining $2, 3, \ldots, p-2$ are set into pairs a and $\tilde{a}$, where $a \neq \tilde{a}$. So if these $\frac{p-3}{2}$ congruences are multiplied, we obtain $2 \cdot 3 \cdots (p-2) \equiv 1(\text{mod } p) \Rightarrow (p-2)! \equiv 1(\text{mod } p) \Rightarrow (p-1)! \equiv (p-1) \equiv -1(\text{mod } p)$. □

Let us illustrate the use of the theorem by means of an example. Let us take

$p = 11$. Divide the integers $2, 3, 4, 5, 6, 7, 8, 9$ into $\frac{p-3}{2}$ pairs such as

$$\begin{aligned} 2 \cdot 6 &\equiv 1(\mod 11) \\ 3 \cdot 4 &\equiv 1(\mod 11) \\ 7 \cdot 8 &\equiv 1(\mod 11) \\ 5 \cdot 9 &\equiv 1(\mod 11) \end{aligned}$$

Multiplying each pair together we obtain, $9! \equiv 1(\mod 11)$. Hence $10! \equiv 1(\mod 11)$, shows the result is true for $p = 11$. An interesting observation is that the converse is also true. Let n be a non–prime required integer. Then n must have a divisor d where $1 < d < n$. As $d \leq n - 1$, we have $d|(n-1)!$. Now from the condition we have, $n|((n-1)!+1)$. Hence combining the conditions, we have $d|((n-1)!+1)$. Thus $d|1$ leads to contradiction, showing n is prime. Taking Wilson's theorem and its converse together we can say that the condition is necessary and sufficient for an integer to be prime. Thus it gives us a condition of testing primality.

Now we are at the end of this discussion with an application of Wilson's theorem on quadratic congruences, where quadratic congruences assume the form $Ax^2 + Bx + C \equiv 0(\mod m)$, where $A \not\equiv 0(\mod m)$ (otherwise the congruence would be a linear congruence). We will learn methods to evaluate these quadratic congruences. However, we will first restrict our modulus m to being only an odd prime $(3, 5, 7, 11, 13, \ldots)$, or rather, any prime except 2. Now we are in a position to state the following theorem:

Theorem 5.4.2. *The quadratic congruence* $x^2 + 1 \equiv 0(\mod p)$ *where* p *is an odd prime, has a solution if and only if* $p \equiv 1(\mod 4)$.

Proof. Let a be a solution of $x^2+1 \equiv 0(\mod p)$ then $a^2 \equiv -1(\mod p)$. Since $p \nmid a$ by Fermat's theorem, we have $1 \equiv a^{p-1}(\mod p) \equiv (a^2)^{\frac{p-1}{2}}(\mod p) \equiv (-1)^{\frac{p-1}{2}}(\mod p)$. The possibility that $p = 4k + 3$ for any integer k does not arise as $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$. Therefore $1 \equiv (-1)(\mod p)$ implies $p|2$ which is a contradiction. So p is of the form $4k + 1$. Now, $(p-1)! = 1 \cdot 2 \cdots \dfrac{p-1}{2} \cdot \dfrac{p+1}{2} \cdots (p-2)(p-1)$ and

$$\begin{aligned} p - 1 &\equiv -1(\mod p) \\ p - 2 &\equiv -2(\mod p) \\ &\vdots \\ \frac{p+1}{2} &\equiv \left(\frac{p-1}{2}\right)(\mod p). \end{aligned}$$

Therefore $(p-1)! \equiv (-1)^{\frac{p-1}{2}}\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod p$. If we assume $p = 4k+1$, then $(-1)^{\frac{p-1}{2}} = 1$. Therefore $-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p$, by Wilson's theorem. Therefore $\left(\frac{p-1}{2}\right)!$ satisfies $x^2 + 1 \equiv 0 (\bmod\ p)$. □

5.5 Worked out Exercises

Problem 5.5.1. *Find the remainder when* $15!$ *is divided by* 17.

Solution 5.5.1. *Since* $(17-1)! = 16!$, *we have by virtue of Wilson's theorem* $(17-1)! \equiv -1 (\bmod\ 17)$. *Therefore* $16! \equiv -1 (\bmod\ 17) \equiv 16 (\bmod\ 17) \Rightarrow 15! \equiv 1 (\bmod\ 17)$. *Hence the remainder is* 1.

Problem 5.5.2. *Find the remainder when* $2(26)!$ *is divided by* 29.

Solution 5.5.2. *From Wilson's theorem, we find* $28! \equiv -1 (\bmod\ 29) \Rightarrow 28! \equiv 28 (\bmod\ 29) \Rightarrow 27! \equiv 1 (\bmod\ 29)$. *Here we note that* $\gcd(28, 29) = 1 \Rightarrow 27(26)! \equiv (1+29) = 30 (\bmod\ 29) \Rightarrow 9(26)! \equiv 10 (\bmod\ 29) \Rightarrow 9(26)! \equiv (10+29) = 9 (\bmod\ 29) \Rightarrow 3(26)! \equiv 13 (\bmod\ 29) \Rightarrow 3(26)! \equiv (13+29) = 42 (\bmod\ 29) \Rightarrow (26)! \equiv 14 (\bmod\ 29)$. *Therefore* $2(26)! \equiv 28 (\bmod\ 29)$. *Thus,* 28 *is the remainder.*

Problem 5.5.3. *Show that* $18! \equiv -1 (\bmod\ 437)$.

Solution 5.5.3. *Note that* $437 = 19 \cdot 23$, *where both* 19 *and* 23 *are prime numbers. By Wilson's theorem, we have* $18! \equiv -1 (\bmod\ 19)$ *therefore* $19 | (18! + 1)$ *holds. So here the only thing we need to show is* $23 | (18! + 1)$, *because* $\gcd(19, 23) = 1$. *Further by Wilson's theorem, we obtain* $22! \equiv -1 (\bmod\ 23) \equiv 22 (\bmod\ 23) \Rightarrow 21! \equiv 1 (\bmod\ 23) \equiv 1 + 23 = 24 (\bmod\ 23) \Rightarrow 7(20)! \equiv 8 (\bmod\ 23) \Rightarrow 7 \cdot 5 \cdot 19! \equiv 2 \equiv 2 + 23 \equiv 25 (\bmod\ 23) \Rightarrow 7 \cdot 19 \cdot 18! \equiv 5 (\bmod\ 23) \equiv 5 + 23 = 28 (\bmod\ 23) \Rightarrow 19 \cdot 18! \equiv 4 (\bmod\ 23) \Rightarrow 19 \cdot 18! \equiv (4 - 23) = -19 (\bmod\ 23) \Rightarrow 18! \equiv -1 (\bmod\ 23)$. *Therefore* $23 \big| (18! + 1) \Rightarrow 437 \big| (18! + 1)$.

Problem 5.5.4. *Prove that for* $n (> 1)$ *is prime if and only if* $(n-2)! \equiv 1 (\bmod\ n)$.

Solution 5.5.4. *By Wilson's theorem and it's converse we have,* n *is prime if and only if* $(n-1)! \equiv -1 (\bmod\ n)$. *Hence* $(n-1)! \equiv -1 + n = n - 1 (\bmod\ n)$. *Therefore* $(n-2)! \equiv 1 (\bmod\ n)$, *as* $\gcd(n, n-1) = 1$.

Problem 5.5.5. *If* n *is composite then show that* $(n-1)! \equiv 0 (\bmod\ n)$ *except* $n = 4$.

Solution 5.5.5. *If* $n = 4$*, then* $(4-1)! = 3! = 6 \equiv 2(\mod 4)$*. Thus this equivalence is not true for* $n = 4$*. If* $n > 4$ *is a composite number, then* $n = r \cdot s$ *for some integers* r *and* s*. Since* $\gcd(n, n-1) = 1$*, therefore* $1 < r < n-1$*. So* r *must be the one of the factor of* $(n-1)!$*. Similarly, for* $1 < s < n-1$ *the above argument is also true.*

If $r \neq s$*, then* r *and* s *are different factors of* $(n-1)!$*. So* $n = r \cdot s|(n-1)!$*. Therefore* $(n-1)! \equiv 0(\mod n)$*.*

If $r = s$*, then* $n = r^2$*. Our claim is* $r < \frac{n}{2}$*. If not then,* $r \geq \frac{n}{2}$*. Therefore* $n = r^2 \geq \frac{n^2}{4} \Rightarrow 4 \geq n$*. But this is not true because* $n > 4$*. Hence* $r < \frac{n}{2} \Rightarrow 2r < n \Rightarrow 2r \leq n-1$*. Both* r *and* $2r$ *are factors of* $(n-1)!$*, therefore* $r(2r)\big|(n-1)! \Rightarrow r^2\big|(n-1)!$*. Hence* $(n-1)! \equiv 0(\mod n)$*.*

Problem 5.5.6. *Given a prime* p*, establish* $(p-1)! \equiv (p-1)(\mod 1+2+3+\cdots+(p-1))$*.*

Solution 5.5.6. *An appeal to Wilson's theorem generates,* $(p-1)! \equiv -1 = p-1(\mod p)$*. Therefore* $p|\{(p-1)!-(p-1)\}$*. We know that,* $1+2+3+\cdots+(p-1) = \dfrac{p(p-1)}{2}$*. Since* $p-1$ *is even, therefore* $\frac{(p-1)}{2}$ *is an integer and* $\frac{(p-1)}{2} < (p-1)$*. Furthermore,* $(p-1)\big|\{(p-1)!-(p-1)\} \Rightarrow \frac{(p-1)}{2}\big|\{(p-1)!-(p-1)\}$*. Because* $\gcd\left(\frac{(p-1)}{2}, p\right) = 1$*, therefore both* p *and* $\frac{(p-1)}{2}$ *divide* $\{(p-1)!-(p-1)\}$*. Thus* $\frac{p(p-1)}{2}\big|\{(p-1)!-(p-1)\} \Rightarrow (p-1)! \equiv (p-1)(\mod 1+2+3\cdots+(p-1))$*.*

Problem 5.5.7. *If* p *is a prime prove that* $p\big|(a^p + (p-1)! \cdot a)$*, for any integer* a*.*

Solution 5.5.7. *Taking into consideration Euler's generalisation theorem and Wilson's theorem, we find* $a^p \equiv a(\mod p)$ *and* $-1 \equiv (p-1)!(\mod p)$ *hold respectively. Multiplying last two congruences, we have* $-a^p \equiv (p-1)! \cdot a(\mod p)$*. This proves,* $p\big|(a^p + (p-1)! \cdot a)$*.*

Problem 5.5.8. *If* p *is a prime prove that* $p|((p-1)! \cdot a^p + a)$*, for any integer* a*.*

Solution 5.5.8. *Hint: Same as Problem(5.5.7)*

Problem 5.5.9. *Verify* $4(29!) + 5!$ *is divided by* 31*.*

Solution 5.5.9. *An appeal to Wilson's theorem gives,* $30! \equiv -1(\mod 31)$*. Therefore* $30 \cdot 29! \equiv 31 - 1 = 30(\mod 31) \Rightarrow 29! \equiv 1(\mod 31)$*. Hence* $4(29)! \equiv 4(\mod 31)$*. Thus, we have* $4(29!) + 5! \equiv 4 + 120 = 124(\mod 31) \equiv 0(\mod 31)$*.*

Problem 5.5.10. *Obtain the solution of* $x^2 \equiv -1(\mod 29)$*.*

Solution 5.5.10. *As* $29 \equiv 1(\bmod 4)$ *so,* $\exists$ *a solution given by* $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1(\bmod p)$*[refer to Theorem 5.4.2]. Therefore* $\pm\left(\frac{29-1}{2}\right)! = \pm 14!$.

Problem 5.5.11. *Prove that the odd prime divisor of* n^2+1 *is of the form* $4k+1$.

Solution 5.5.11. *Let* p *be an odd prime divisor of* n^2+1*. Therefore* $n^2+1 \equiv 0(\bmod p)$*. So* n *satisfies the quadratic congruence equation* $x^2 \equiv -1(\bmod p)$*. Hence* p *is of the form* $4k+1$*. Because* p *is of the form* $4k+3$ *it follows that,* $n^2 \equiv -1(\bmod p) \Rightarrow 1 \equiv n^{p-1}(\bmod p) \equiv (n^2)^{\frac{p-1}{2}}(\bmod p) \equiv (-1)^{\frac{p-1}{2}}(\bmod p) \Rightarrow 1 \equiv (-1)^{\frac{4k+3-1}{2}}(\bmod p) \equiv (-1)^{2k+1}(\bmod p) \equiv -1(\bmod p)$*. This proves* $p \big| 2$*, a contradiction.*

5.6 Exercises:

1. Verify using Fermat's theorem: $17 \big| (11^{104}+1)$.
2. Find the remainder of 97! when divided by 101.
3. Derive the congruence: $a^{13} \equiv a(\bmod 3 \cdot 7 \cdot 13)$ for all integer a.
4. Find the remainder of 53! when divided by 61.
5. Prove $1835^{1910} + 1986^{2061} \equiv 0(\bmod 7)$.
6. Assume $p \nmid a, p \nmid b$, p is prime;
   (i) If $a^p \equiv b^p(\bmod p)$ then, $a \equiv b(\bmod p)$.
   (ii) If $a^p \equiv b^p(\bmod p)$ then, $a^p \equiv b^p(\bmod p^2)$.
7. Using Fermat's theorem, prove that for a odd prime p;
   (i) $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1(\bmod p)$.
   (ii) $1^p + 2^p + \cdots + (p-1)^p \equiv 0(\bmod p)$
8. Confirm that the followings are absolute prime: (a) $2821 = 7 \cdot 13 \cdot 31$ (b) $2465 = 5 \cdot 17 \cdot 29$.
9. Use Korselt's criterion to determine which of them are Charmichael numbers: (a) 8911 (b) 10659 (c) 162401 (d) 126217.
10. Find the remainder when 3^{456} is divided by 7.
11. Find all positive integers n such that 2^{2^n+1} is divided by 17.

12. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 17$.
13. Determine whether 17 is a prime or not using Wilson's theorem.
14. If p and $p + 2$ are a pair of primes then prove that $4((p-1)! + 1) + p \equiv 0(\bmod p(p+2))$.
15. What is the remainder of 149! when divided by 139.
16. Find all Carmichael numbers of the form $5pq$ where p and q are primes.
17. Find a Carmichael number of the form $7 \cdot 23 \cdot q$ where q is an odd prime.
18. Show that 1373653 is a strong pseudoprime to base $2,\ 3$.
19. Obtain the solution of $x^2 \equiv -1(\bmod 37)$.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

6

Arithmetic Functions

> *"Mathematics is the queen of sciences and number theory is the queen of mathematics."*
>
> – Carl Friedrich Gauss

6.1 Introduction

There are few functions of special importance in connection with the study of the divisors of an integer. Any function whose domain of definition is the set of integers is known as the arithmetic function.

Present chapter treats multiplicative functions defined on integers, having the property that there is value at the product of two relatively prime integers equal to the product of the value of the function at these integers. In this chapter several results about multiplicative functions are done that will be used later on. We also define the sum of divisors and the number of divisors functions. Later on the Mӧbius functions investigate integers in terms of their prime decomposition. The summatory function of a given function takes the sum of the values of f at the divisors of a given integer a. The Mӧbius inversion formula is determined, which writes the values of f in terms of the values of its summatory function. We conclude the chapter by presenting the Greatest Integer function along with some interesting properties.

6.2 The Sum and Number of Divisors

In mathematics, function has an important role to play with different topics. For advance study of number theory we have some important aspects related to functions. Any function whose domain is the set of integers are called the number theoretic function or arithmetic functions. The range set may be other than positive integers also. We will start our discussions with the sum and number of divisors.

Definition 6.2.1. *Given a positive integer n, $\tau(n)$ is defined as total number of positive divisors of n.*

For an example if we choose $n = 12$, then $\tau(12) = 6$ as the divisors are $1, 2, 3, 4, 5, 6, 12$. In the following table we have shown few integers and their corresponding number of divisors.

n	2	3	4	5	6	7	8	9	10
$\tau(n)$	2	2	3	2	4	2	4	3	4

Definition 6.2.2. *Given a positive integer n, $\sigma(n)$ is defined as the sum of their divisors.*

For example if we choose $n = 12$, then $\sigma(12) = 1+2+3+4+5+6+12 = 28$. In the following table we have shown few integers and their corresponding sum of divisors.

n	2	3	4	5	6	7	8	9	10
$\sigma(n)$	3	4	7	6	12	8	15	13	18

Before going for further discussions we are going to interpret the symbol $\sum_{d|n} f(d)$ which means 'Sum of values of $f(d)$ as d runs over all positive divisors of n'. This sum is denoted as $F(n)$ and defined as $F(n) = \sum_{d|n} f(d)$. If n is prime then $\tau(n) = 2$ and $\sigma(n) = n + 1$. The converse is also true is justified with the given example: $\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$ i.e. $\tau(n) = \sum_{d|n} 1, \sigma(n) = \sum_{d|n} d$, therefore, $\tau(10) = \sum_{d|10} 1 = 1 + 1 + 1 + 1 + 1 = 4$ and $\sigma(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18$. Those are already shown in the above two given tables.

The first theorem of the chapter aims to find the positive divisors of a positive integer where the prime factorisation of that positive integer is already known.

Theorem 6.2.1. *If* $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$ *is the prime factorization of* $n > 1$, *then the positive divisors of* n *are precisely, those integers* d *of the form* $d = p_1^{b_1} p_1^{b_1} \cdots p_1^{b_r}$, *where* $0 \leq b_i \leq t_i (i = 1, 2, 3, \ldots r)$ *and vice–versa.*

Proof. If $d = 1$, then $b_1 = b_2 = \cdots = b_r = 0$ and $d = n$, then $b_1 = t_1, \ldots, b_r = t_r$. Let $n = dd'$ where $d, d' > 1$ holds. Then they can be expressed as product of primes where $d = q_1 q_2 q_3 \ldots q_s$, $d' = r_1 r_2 r_3 \ldots r_u$ considering q_i, r_j as primes. Hence $p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} = q_1 q_2 q_3 \ldots q_s r_1 r_2 r_3 \ldots r_u$. By uniqueness of primes some of q_i is same as p_j so collecting them we have, $d = q_1 q_2 q_3 \ldots q_s = p_1^{b_1} \cdots p_1^{b_r}$ where $b_i = 0$ is possible.

Conversely, every number $d = p_1^{b_1} p_1^{b_1} \cdots p_1^{b_r}$ turns out to be the divisor of n. Then we have, $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r} = (p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r})(p_1^{t_1 - b_1} p_2^{t_2 - b_2} \cdots p_r^{t_r - b_r}) = dd'$ where $d' = p_1^{t_1 - b_1} p_2^{t_2 - b_2} \cdots p_r^{t_r - b_r}$ and $t_i - b_i \geq 0$ for all i, then $d' > 0$ and $d | n$.

The next theorem deals with the formula for both the number theoretic functions $\tau(n)$ and $\sigma(n)$. The previous two tables on these two functions illustrate, if the integer n is prime then $\tau(n) = 2$ and $\sigma(n) = n + 1$. In particular if $n = p^\alpha$ where p is prime then the divisors of p^α are $1, p, p^2 \cdots p^\alpha$ thus $\tau(p^\alpha) = \alpha + 1$ and $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \dfrac{p^{\alpha+1} - 1}{p - 1}$. Thus the general formula for these two functions are as follows. □

Theorem 6.2.2. *If* $n = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}$ *is prime factorization of* $r > 1$ *then the followings are true.*

1. $\tau(n) = (t_1 + 1)(t_2 + 1)(t_3 + 1) \ldots (t_r + 1)$.

2. $\sigma(n) = \dfrac{p_1^{t_1+1} - 1}{p_1 - 1} \dfrac{p_2^{t_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{t_r+1} - 1}{p_r - 1}$.

Proof. 1. According to the above theorem, the positive divisors of n are precisely those integers $d = p_1^{b_1} p_1^{b_1} \cdots p_1^{b_r}$ where $0 \leq b_i \leq t_i$ holds. So there are $t_1 + 1$ choices for $b_1, (t_2 + 1)$ choices for b_2 and continuing we have $t_r + 1$ choices for b_r. Therefore total number of positive divisors are $(t_1 + 1)(t_2 + 1)(t_3 + 1) \ldots (t_r + 1)$. Hence $\tau(n) = (t_1 + 1)(t_2 + 1)(t_3 + 1) \cdots (t_r + 1) = \sum\limits_{1 \leq j \leq r} (t_j + 1)$.

2. In order to evaluate $\sigma(n)$ we consider the product, $(1 + p_1 + p_1^2 + p_1^3 + \ldots p_1^{t_1})(1 + p_2^2 + p_2^3 + \ldots p_2^{t_2}) \cdots (1 + p_r + p_r^2 + \ldots p_r^{t_r})$ where each term in

brackets are positive divisor of each prime factorisation of n. Therefore

$$\begin{aligned}\sigma(n) &= (1+p_1+p_1^2+p_1^3+\ldots p_1^{t_1})(1+p_2^2+p_2^3+\ldots p_2^{t_2})\cdots(1+p_r+p_r^2+\ldots p_r^{t_r})\\ &= \frac{p_1^{t_1+1}-1}{p_1-1}\frac{p_2^{t_2+1}-1}{p_2-1}\cdots\frac{p_r^{t_r+1}-1}{p_r-1}\\ &= \prod_{1\le i\le r}\frac{p_i^{t_i+1}-1}{p_i-1}.\end{aligned}$$

□

We illustrate this with an example.

Example 6.2.1. *Let* $n = 150 = 2\times3\times5^2$ *then* $\tau(150) = (1+1)(1+1)(2+1) = 12$ *and* $\sigma(150) = \dfrac{2^2-1}{2-1}\dfrac{3^2-1}{3-1}\dfrac{5^3-1}{5-1} = 372.$

Now the following definition deals with a special property of number theoretic functions known to be multiplicative property:

Definition 6.2.3. *A number theoretic function f is said to be multiplicative if, for positive integers m and n, $f(mn) = f(m)f(n)$ where* $\gcd(m,n) = 1$.

Remark 6.2.1. *The function $f(n) = 1$, $\forall\ n \in \mathbb{Z}$ is multiplicative because $f(mn) = 1$, $f(m) = 1$ & $f(n) = 1$, so that $f(mn) = f(m)f(n)$. Similarly, the identity function $g(n) = n$, $\forall\ n \in \mathbb{Z}$ is multiplicative, since $g(mn) = mn = g(m)g(n)$. Observe that multiplicative functions f and g with the property $f(mn) = f(m)f(n)$ and $g(mn) = g(m)g(n)$ for all pairs of integers m and n, whether or not* $\gcd(m,n) = 1$, *is said to be completely multiplicative functions.*

Now we are at the stage to discuss the multiplicative property of τ and σ.

Theorem 6.2.3. *The functions τ and σ are both multiplicative.*

Proof. Let m and n be two relatively prime integers both greater than 1, for if any one of them is 1 then the result is trivial. So our primal assumption is both $m, n > 1$. Let $m = p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$ and $n = q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ be prime factorisation of m and n respectively where no $p_i = q_r$ because $\gcd(m,n) = 1$ and if any of p_i's same as any of q_r's then this leads to a contradiction(Why!). Therefore $mn = p_1^{t_1}p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ and

$$\begin{aligned}\tau(mn) &= [(t_1+1)(t_2+1)\cdots(t_r+1)][(j_1+1)(j_2+1)\cdots(j_s+1)]\\ &= \tau(m)\tau(n)\\ \sigma(mn) &= \prod_{1\le i\le r}\frac{p_i^{t_i+1}-1}{p_i-1}\prod_{1\le j\le s}\frac{q_i^{j_s+1}-1}{q_s-1}\\ &= \sigma(m)\sigma(n).\end{aligned}$$

□

We will continue our study on multiplicative functions of positive divisors for products of relatively prime integers. Next lemma is the first step on this study.

Lemma 6.2.1. *If* $\gcd(m,n)=1$*, then the set of positive divisors of* mn *consists of all products* d_1d_2 *where* $d_1|m$ *and* $d_2|n$ *and* $\gcd(d_1,d_2)=1$*.*

Proof. Let us assume $m,n>1$ and $m=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$ and $n=q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}$ be their respective prime factorization. Therefore

$$mn=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}q_1^{j_1}q_1^{j_1}q_2^{j_2}\cdots q_s^{j_s}.$$

Hence any positive divisors d of mn represented in the form

$$d=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}q_1^{b_1}q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s},$$

where, $0\le a_i\le t_i$ and $0\le b_i\le j_i$ then $d=d_1d_2$ where $d_1=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ where $d_1|m$ and $d_2=q_1^{b_1}q_1^{b_1}q_2^{b_2}\cdots q_s^{b_s}$ where $d_2|n$ and $\gcd(d_1,d_2)=1$, as $p_i\neq q_j$ because m and n are relatively prime. □

Before proceeding further we will illustrate the idea of a positive divisor by means of an example. Let $m=4$ and $n=5$. Also $F(n)=\sum_{d|n}f(d)$ is defined earlier in this section. Here we choose f as an arithmetic function. In this example we will show $F(20)=F(4)F(5)$. Now the divisors of 20 are $1,2,4,5,10,20$, therefore $F(20)=f(1)+f(2)+f(4)+f(5)+f(10)+f(20)$. Also the divisors of 4 are $1,2,4$ and of 5 are $1,5$. Thus we have,

$$\begin{aligned}
F(20)&=f(1)+f(2)+f(4)+f(5)+f(10)+f(20)\\
&=f(1\cdot 1)+f(1\cdot 2)+f(1\cdot 4)+f(1\cdot 5)+f(2\cdot 5)+f(4\cdot 5)\\
&=f(1)f(1)+f(1)f(2)+f(1)f(4)+f(1)f(5)+f(2)f(5)+f(4)f(5)\\
&=(f(1)+f(2)+f(4))(f(1)+f(5))\\
&=F(4)F(5)
\end{aligned}$$

This shows the arithmetic function F is multiplicative. Now the theorem is as follows,

Theorem 6.2.4. *If* f *is a multiplicative function and* F *is defined by* $F(n)=\sum_{d|n}f(d)$ *then* F *is also multiplicative.*

Proof. Let m, n are relatively prime integer then

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2),$$

where $\gcd(d_1, d_2) = 1$ and f is multiplicative, then we have $f(d_1 d_2) = f(d_1)f(d_2)$. Therefore

$$F(mn) = \sum_{d_1|m, d_2|n} f(d_1)f(d_2) = \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) = F(m)F(n).$$

This proves the fact that F is multiplicative. □

6.3 Worked out Exercises

Problem 6.3.1. *Prove that there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.*

Solution 6.3.1. *There are infinitely many integers k such that* $\gcd(k, 10) = 1$. *Let us consider $m = 5k, n = 4k$. This implies there exist infinitely many such m, n. Suppose k is prime with $k \neq 2, 5$. Now $m^2 = 5^2k^2$ and $n^2 = 4^2k^2 = 2^4k^2$. Theorem 6.2.2 yields*

$$\sigma(m^2) = \frac{5^3 - 1}{5 - 1} \cdot \frac{k^3 - 1}{k - 1} = 31\left(\frac{k^3 - 1}{k - 1}\right).$$
$$\sigma(n^2) = \frac{2^5 - 1}{2 - 1} \cdot \frac{k^3 - 1}{k - 1} = 31\left(\frac{k^3 - 1}{k - 1}\right).$$

Thus there are infinitely many pairs of integers m and n with $\sigma(m^2) = \sigma(n^2)$.

Problem 6.3.2. *If n is a square-free integer, prove that $\tau(n) = 2^s$, where s is the number of prime divisors of n.*

Solution 6.3.2. *Since n is square-free, therefore $n = p_1 p_2 \cdots p_r$ where each $p_i \neq p_j \neq$ for $i \neq j$. From Theorem 6.2.2, we obtain*

$$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_s + 1), \text{ with } k_i = 1 \text{ for all } i.$$

Thus $\tau(n) = (1 + 1)(1 + 1) \cdots (1 + 1) = 2 \cdot 2 \cdots 2 = 2^s$ as there are s terms

Problem 6.3.3. *Prove that the following statements are equivalent:*

1. *$\tau(n)$ is an odd integer.*

2. n is a perfect square.

Solution 6.3.3. *1⇒2:Suppose (1) holds. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Then using Theorem 6.2.2, we have $\tau(n) = (k_1+1)(k_2+1)\cdots(k_s+1)$. Note that each k_i+1 is odd, so k_i is even. Hence $k_i = 2j_i$ implies*

$$n = p_1^{2j_1} p_2^{2j_2} \cdots p_s^{2j_s} = (p_1^{j_1} p_1^{j_2} \cdots p_s^{j_s})^2,$$

which proves n is a perfect-square.

2⇒1:Suppose (2) holds. Then $n = a^2$ for some $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, which implies

$$n = p_1^{2k_1} p_2^{2k_2} \cdots p_s^{2k_s}.$$

Therefore $\tau(n) = (2k_1+1)(2k_2+1)\cdots(2k_s+1)$. Since each of $2k_i+1$ is odd, therefore $\tau(n)$ is odd.

Problem 6.3.4. *For any positive integer z, prove $\sum_{d|z} \frac{1}{d} = \frac{\sigma(z)}{z}$.*

Solution 6.3.4. *Note that d is a divisor of z if and only if $\frac{z}{d}$ is a divisor of z(Why!). Therefore the set of divisors of z are given by $\{d_1, d_2, \ldots, d_s\}$, which further can be expressed as $\left\{\frac{z}{d_1}, \frac{z}{d_2}, \ldots, \frac{z}{d_s}\right\}$. Thus*

$$\sigma(z) = d_1 + d_2 + \ldots + d_s = \frac{z}{d_1} + \frac{z}{d_2} + \ldots + \frac{z}{d_s} = z\left(\frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_s}\right),$$

implies

$$\frac{\sigma(z)}{z} = \frac{1}{d_1} + \frac{1}{d_2} + \ldots + \frac{1}{d_s} = \sum_{d|z} \frac{1}{d}.$$

Problem 6.3.5. *If $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ is the prime factorization of $z > 1$, then prove that*

$$1 > \frac{z}{\sigma(z)} > \left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\cdots\left(1 - \frac{1}{q_s}\right).$$

Solution 6.3.5. *Since the divisors of z include 1 and z, therefore*

$$\sigma(z) \geq z + 1 > z \Rightarrow \frac{z}{\sigma(z)} < 1.$$

By virtue of Theorem 6.2.2, we obtain

$$\sigma(z) = \frac{q_1^{t_1+1} - 1}{q_1 - 1} \frac{q_2^{t_2+1} - 1}{q_2 - 1} \cdots \frac{q_s^{t_s+1} - 1}{q_s - 1}.$$

Therefore

$$\begin{aligned}
\frac{z}{\sigma(z)} &= \frac{q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}}{\frac{(q_1^{t_1+1}-1)(q_2^{t_2+1}-1)\cdots(q_s^{t_s+1}-1)}{(q_1-1)(q_2-1)\cdots(q_s-1)}} \\
&= \frac{(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s})(q_1-1)(q_2-1)\cdots(q_s-1)}{(q_1^{t_1+1}-1)(q_2^{t_2+1}-1)\cdots(q_s^{t_s+1}-1)} \\
&= \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{\frac{(q_1^{t_1+1}-1)(q_2^{t_2+1}-1)\cdots(q_s^{t_s+1}-1)}{q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}}} \\
&= \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{\left(q_1 - \frac{1}{q_1^{t_1}}\right)\left(q_2 - \frac{1}{q_2^{t_2}}\right)\cdots\left(q_s - \frac{1}{q_s^{t_s}}\right)}. \qquad (6.3.1)
\end{aligned}$$

But

$$q_i > q_i - \frac{1}{q_i^{t_i}} \Rightarrow \frac{1}{q_i - \frac{1}{q_i^{t_i}}} > \frac{1}{q_i}.$$

Thus (6.3.1) yields,

$$\begin{aligned}
\frac{z}{\sigma(z)} &= \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{\left(q_1 - \frac{1}{q_1^{t_1}}\right)\left(q_2 - \frac{1}{q_2^{t_2}}\right)\cdots\left(q_s - \frac{1}{q_s^{t_s}}\right)} \\
&> \frac{(q_1-1)(q_2-1)\cdots(q_s-1)}{q_1 q_2 \cdots q_s} \\
&= \left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_s}\right).
\end{aligned}$$

Hence

$$1 > \frac{z}{\sigma(z)} > \left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_s}\right).$$

Problem 6.3.6. *Prove if $z > 1$ is a composite number, then $\sigma(z) > z + \sqrt{z}$.*

Solution 6.3.6. *Since*

$$\sigma(z) = 1 + d_1 + d_2 + \ldots + d_s + z,$$

its suffices to show that

$$d_1 + d_2 + \ldots + d_s > \sqrt{z}.$$

Since z is composite, there exists d_i (for some i) such that $1 < d_i < z$ and $d_i | z$. Therefore $\frac{z}{d_i} | z$ and $d_i < z$ together implies $1 < \frac{z}{d_i}$ and $1 < d_i \Rightarrow \frac{1}{d_i} < 1 \Rightarrow \frac{z}{d_i} < z$. Therefore

$$1 < \frac{z}{d_i} < z.$$

Now two cases may arise:

Case(i) *If* $d_i > \sqrt{z}$*, then clearly* $1 + d_i > \sqrt{z}$*. So*

$$\sigma(z) = 1 + d_1 + d_2 + \ldots + d_s + z > z + \sqrt{z}.$$

Case(ii) *If* $d_i \leq \sqrt{z}$*, then*

$$\frac{1}{\sqrt{z}} \leq \frac{1}{d_i} \Rightarrow \sqrt{z} = \frac{z}{\sqrt{z}} \leq \frac{z}{d_i}.$$

Let $d_j = \dfrac{z}{d_i}$*. Then* $d_j | z$ *implies* $d_j \geq \sqrt{z}$*. Therefore* $1 + d_j + z > z + \sqrt{z}$*. Hence from* $\sigma(z) = 1 + d_1 + d_2 + \ldots + d_s + z$*, it follows* $\sigma(z) > z + \sqrt{z}$*.*

Thus combining the above cases the assertion follows.

Problem 6.3.7. *For any integer* $k > 1$*, show that*

1. *there exist infinitely many integers* n *for which* $\tau(n) = k$*,*
2. *but at most finitely many* n *with* $\sigma(n) = k$*.*

Solution 6.3.7. 1. *Let* p *be any prime and* $n = p^{k-1}$*. Then* $\tau(n) = k$ *(How!). Since there are infinitely many primes, therefore there are infinitely many* n *satisfying* $n = p^{k-1}$ *and* $\tau(n) = k$*.*

2. *Using Problem (6.3.5), we have* $\sigma(n) > n$*,* $\forall n$*. If* $\sigma(n) = k$*, for any* k*, then* k *serves as an upper bound to* n*. In fact, for any* $n \geq k$*,* $\sigma(n) > k$ *(How!). Hence there are at most* $k (> 1)$ *integers such that* $\sigma(n) \leq k$*.*

Problem 6.3.8. *If pair of successive odd integers* q *and* $q + 2$ *that are both primes, called twin primes. For these* q *and* $q + 2$ *prove that* $\sigma(q + 2) = \sigma(q) + 2$*.*

Solution 6.3.8. *The only divisors for any prime* q *are* 1 *and* q *itself. Therefore* $\sigma(q) = q + 1$*. Thus* $\sigma(q + 2) = q + 3$ *and* $\sigma(q) + 2 = q + 3$*. Thus* q *and* $q + 2$ *together implies* $\sigma(q + 2) = \sigma(q) + 2$*.*

Problem 6.3.9. *Let* f *and* g *be multiplicative functions that are not identically zero and have the property that* $f(p^k) = g(p^k)$ *for each prime* p *and* $k \geq 1$*. Prove that* $f = g$*.*

Solution 6.3.9. *Let* $n > 1$ *be an arbitrary integer with prime factorization given by* $n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$*. Then*

$$\begin{aligned} f(n) &= f(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}) \\ &= f(q_1^{t_1}) f(q_2^{t_2}) \cdots f(q_s^{t_s}) \\ &= g(q_1^{t_1}) g(q_2^{t_2}) \cdots g(q_s^{t_s}) \\ &= g(q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}) \\ &= g(n). \end{aligned}$$

In particular, if $n = 1$ then $f(1) = g(1) = 1$. Hence combining all $f = g$ holds.

Problem 6.3.10. *For any integer $z > 1$, prove that there exist integers z_1 and z_2 for which $\tau(z_1) + \tau(z_2) = z$.*

Solution 6.3.10. *If z is prime, then $\tau(z) = 2$. Since $tau(1) = 1$, taking $z_1 = z_2 = 1$ gives $\tau(z_1) + \tau(z_2) = \tau(z)$.*

If z is composite, let $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be its prime factorization. Then at least one of $t_i \geq 2$. Let $q_j^{t_j}$ be that factor. Therefore

$$\begin{aligned}\tau(z) &= (t_1 + 1)(t_2 + 1) \cdots (t_j + 1) \cdots (t_s + 1)\\ &= t_j(t_1 + 1)(t_2 + 1) \cdots (t_s + 1) + (t_1 + 1)(t_2 + 1) \cdots (t_s + 1).\end{aligned}$$

Let $z_1 = q_1^{t_1} q_2^{t_2} \cdots q_j^{t_{j-1}} \cdots q_s^{t_s}$ and $z_2 = \dfrac{z}{q_j^{t_j}} = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$, where $q_i \neq q_j$. Hence

$$\begin{aligned}\tau(z_1) &= (t_1 + 1)(t_2 + 1) \cdots (t_j - 1 + 1) \cdots (t_s + 1)\\ &= t_j(t_1 + 1)(t_2 + 1) \cdots (t_s + 1).\\ \tau(z_2) &= (t_1 + 1)(t_2 + 1) \cdots (t_s + 1).\end{aligned}$$

Combining we obtain, $\tau(z_1) + \tau(z_2) = \tau(z)$.

Problem 6.3.11. *For any integer $z \geq 1$, prove that $\sum_{d|z} \tau(d)^3 = \big(\sum_{d|z} \tau(d)\big)^2$.*

Solution 6.3.11. *Since $\tau(z)$ is a multiplicative function, therefore $[\tau(mn)]^3 = [\tau(m)\tau(z)]^3 = [\tau(m)]^3[\tau(z)]^3$. This shows $\tau(z)^3$ is a multiplicative function. Hence by virtue of Theorem 6.2.4, $F(z) = \displaystyle\sum_{d|z} \tau(d)^3$ is multiplicative. Moreover, the multiplicative property of $G(z) = \sum_{d|z} \tau(d)$ implies $H(z) = G(z)^2$ is multiplicative(Why!).*

Let $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be its prime factorization. Since F and H both are multiplicative, for $z = q^t$, $F(z) = H(z)$ holds. By similar reasoning, the relation $F(z) = H(z)$ holds true for $z = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$. Therefore considering $z = q^t$ and applying Theorem 6.2.1, all the divisors of z are given by $1, q, q^2, \ldots, q^t$. Thus

$$\begin{aligned}\sum_{d|q^t}\tau(d)^3 &= \tau(1)^3+\tau(q)^3+\ldots+\tau(q^t)^3\\ &= 1+(1+1)^3+(2+1)^3+\ldots+(t+1)^3\\ &= 1+2^3+3^3+\ldots+(t+1)^3\\ &= \left[\frac{(t+1)(t+2)}{2}\right]^2.\\ \Big(\sum_{d|q^t}\tau(d)\Big)^2 &= [\tau(1)+\tau(q)+\ldots+\tau(q^t)]^2\\ &= [1+(1+1)+(2+1)+\ldots+(t+1)]^2\\ &= \left[\frac{(t+1)(t+2)}{2}\right]^2.\\ \textit{Hence}\ \sum_{d|q^t}\tau(d)^3 &= \Big(\sum_{d|q^t}\tau(d)\Big)^2,\ \ \textit{so}\ \ F(z)=H(z)\ \ \textit{for}\ \ z=q^t.\end{aligned}$$

Problem 6.3.12. *Given $z \geq 1$, let $\sigma_s(z)$ denote the sum of the sth powers of the positive divisors of z; that is, $\sigma_s(z) = \sum_{d|z} d^s$. Prove that*

$$\sigma_s(z) = \left(\frac{q_1^{s(t_1+1)}-1}{q_1^s-1}\right)\left(\frac{q_2^{s(t_2+1)}-1}{q_2^s-1}\right)\cdots\left(\frac{q_r^{s(t_1+1)}-1}{q_r^s-1}\right),$$

$z = q_1^{t_1}q_2^{t_2}\cdots q_r^{t_r}$ being the prime factorization of z.

Solution 6.3.12. *By virtue of Theorem 6.2.1, all divisors of z are of the form*

$$q_1^{a_1}q_2^{a_2}\ldots q_r^{a_r},\ 0 \leq a_i \leq t_i.$$

Therefore all the sth powers of the divisors of z are of the form

$$q_1^{a_1 s}q_2^{a_2 s}\ldots q_r^{a_r s}.$$

Let us consider the product of sums

$$(1+q_1^s+q_1^{2s}+q_1^{t_1 s})\ldots(1+q_r^s+q_r^{2s}+q_r^{t_r s}).$$

Each positive divisor to the sth power occurs only once as a term in the expansion of the product. Therefore

$$\sigma_s(z) = (1+q_1^s+q_1^{2s}+q_1^{t_1 s})\ldots(1+q_r^s+q_r^{2s}+q_r^{t_r s}).$$

Applying the formulae for the sum of the finite geometric series,

$$(1+q_i^s+q_i^{2s}+q_i^{t_1 s})=\left(\frac{q_i^{s(t_i+1)}-1}{q_i^s-1}\right),$$

$$\Rightarrow \sigma_s(z)=\left(\frac{q_1^{s(t_1+1)}-1}{q_1^s-1}\right)\left(\frac{q_2^{s(t_2+1)}-1}{q_2^s-1}\right)\cdots\left(\frac{q_r^{s(t_1+1)}-1}{q_r^s-1}\right).$$

Problem 6.3.13. *For any positive integer z, show that*

$$\sum_{d|z}\sigma(d)=\sum_{d|z}\frac{z}{d}\tau(d).$$

Solution 6.3.13. *Let $H(n)=\sum_{d|z}\frac{z}{d}\tau(d)$. Then*

$$\begin{aligned}
G(mn) &= \sum_{d|mn}\frac{mn}{d}\tau(d)\\
&= \sum_{d_1|m,d_2|n}\frac{mn}{d_1d_2}\tau(d_1d_2)\\
&= \sum_{d_1|m,d_2|n}\frac{mn}{d_1d_2}\tau(d_1)\tau(d_2)\\
&= \sum_{d_1|m,d_2|n}\frac{m}{d_1}\tau(d_1)\frac{n}{d_2}\tau(d_2),\ \textit{since } \tau(d) \textit{ is multiplicative}\\
&=\Big(\sum_{d_1|m,d_2|n}\frac{m}{d_1}\tau(d_1)\Big)\Big(\sum_{d_1|m,d_2|n}\frac{n}{d_2}\tau(d_2)\Big)\\
&= G(m)G(n).
\end{aligned}$$

Hence G is a multiplicative function. Using multiplicative property of $\sigma(d)$ the function $F(n)=\sum_{d|z}\sigma(d)$ is multiplicative.

Next let $z=q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s}$ be its prime factorization. To prove

$$\begin{aligned}
F(z) &= F(q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s})\\
&= F(q_1^{t_1})F(q_2^{t_2})\cdots F(q_s^{t_s})\\
&= G(q_1^{t_1})G(q_2^{t_2})\cdots G(q_s^{t_s})\\
&= G(q_1^{t_1}q_2^{t_2}\cdots q_s^{t_s})\\
&= G(z),
\end{aligned}$$

its suffices to show $F(q^t) = G(q^t)$. *Now*

$$\begin{aligned} F(q^t) &= \sum_{d|q^t} \sigma(d) \\ &= q^0 + (q^0 + q^1) + \ldots + (q^0 + q^1 + \ldots + q^s) \\ &= (t+1)q^0 + tq^1 + \ldots + (1)q^t \\ &= (1)q^t + \cdots + tq^1 + (t+1). \qquad (6.3.2) \\ G(q^t) &= \sum_{d|q^t} \frac{q^t}{d}\tau(d) \\ &= \frac{q^t}{q^0}\tau(q^0) + \frac{q^t}{q^1}\tau(q^1) + \ldots + \frac{q^t}{q^t}\tau(q^t) \\ &= (1)q^t + 2q^{t-1} + \ldots + tq + (t+1) \\ &= F(q^t), \text{ by (6.3.2).} \end{aligned}$$

Problem 6.3.14. *For any integer* $z \geq 1$, *prove that* $\tau(z) \leq 2\sqrt{z}$.

Solution 6.3.14. *If* $d|z$, *then either* $d \leq \sqrt{z}$ *or* $\frac{z}{d} \leq \sqrt{z}$. *For if* $d > \sqrt{z}$ *or* $\frac{z}{d} > \sqrt{z}$, *then*

$$d \cdot \frac{z}{d} = z > \sqrt{z}\sqrt{z} = z,$$

a contradiction. Let $d_1, d_2, \ldots, d_t$ *be the divisors of* z *where* $d_1 < d_2 < \ldots < d_t$. *Clearly,* $d_1 = 1, d_t = z$. *Now* $d_i|z \Rightarrow z|d_i$ *and so* $z|d_i$ *must be one of* d_i. *pairing the divisors in such a way that* $d_i d_j = z$, *where* $d_j = z|d_i$. *So either* $d_i \leq d_j$ *or* $d_i \geq d_j$.

Case(i) *t is even: Then we have* $\frac{t}{2}$ *unique pairs* $\{d_i, d_j\}(d_i \neq d_j)$ *such that* $d_i d_j = z$. *Let us arrange every pair in such a way that* $d_i < d_j$. *Let* $d_{t'}$ *be the largest of the* d_i. *Since there are* $\frac{t}{2}$ *unique pairs, it must be* $\frac{t}{2} \leq d_{t'}$. *But* $\tau(z) = t$ *and from above* $d_{t'} \leq \sqrt{z}$. *Thus,*

$$\frac{\tau(z)}{2} \leq \sqrt{z} \Rightarrow \tau(z) \leq 2\sqrt{z}.$$

Case(ii) *t is odd: Then we have* $\frac{t-1}{2}$ *unique pairs* $\{d_i, d_j\}(d_i \neq d_j)$ *such that* $d_i d_j = z$ *and one pair* $\{d_r, d_r\}$ *where* $d_r d_r = z$. *Let us arrange every unique pair in such a way that* $d_i < d_j$. *Let* $d_{t'}$ *be the largest of the* d_i. *Now if* $d_r < d_{t'}$, *considering the pair* $\{d_j, d_{t'}\}$ *and applying the definition of* $d_{t'}$, *we obtain*

$$d_{t'} < d_j, \text{ and } d_{t'} d_j = z.$$

Hence $d_r < d_j \Rightarrow d_r d_r < d_r d_j \Rightarrow z < z$, *a contradiction. Hence* $d_r > d_{t'}$. *But* $d_r^2 = z \Rightarrow d_r = \sqrt{z}$. *As in Case(i),*

$$\frac{t-1}{2} \leq d_{t'} \text{ and } t = \tau(z).$$

Therefore

$$\frac{\tau(z)-1}{2} \leq d_{t'} < d_r = \sqrt{z},$$

which further implies

$$\frac{\tau(z)-1}{2} \leq \sqrt{z}, \tau(z) - 1 < 2\sqrt{z} \Rightarrow \tau(z) \leq 2\sqrt{z}.$$

Hence $\tau(z) \leq 2\sqrt{z}$ *for both even and odd cases.*

Problem 6.3.15. *Find the form of all positive integers* n *satisfying* $\tau(n) = 10$. *What is the smallest positive integer for which this is true?*

Solution 6.3.15. *Let* $n = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ *be the prime factorization of* n. *Then* $\tau(n) = (t_1+1)(t_2+1)\ldots(t_s+1)$. *If* $\tau(n) = 10$, *then the possibilities are* 10 *and* 5×2. *This implies* $t_1 + 1 = 10$ *or* $(t_1+1)(t_2+1) = 5 \times 2$. *Thus* $n = q_1^9$ *or* $n = q_1^4 q_2$ *where* q_1, q_2 *are distinct primes.*

The smallest of such integers would be 2^9 *or* $2^4 \times 3$ *or* $3^4 \times 2$. *Then the smallest among them is* $2^4 \times 3 = 48$.

6.4 Mobi*ü*s μ-function

In this article, we will discuss an important arithmetic function called Mobi*ü*s μ-function with some of its properties.

Definition 6.4.1. *For a positive integer* n, *define* μ *by the rules*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } p^2 | n \text{ for some prime } p; \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i\text{'s are distinct primes.} \end{cases}$$

For example we see that $\mu(2) = -1, \mu(3) = -1, \mu(4) = 0$. Thus if we choose $n = 15 = 3 \times 5$ then $\mu(15) = \mu(3 \cdot 5) = (-1)^2 = 1$. Now in the next theorem we are going to discuss the multiplicative property on Mobiöus μ function.

Theorem 6.4.1. *The function* μ *is a multiplicative function.*

Proof. Its suffices to show that for any two relatively prime integers m and n, $\mu(mn) = \mu(m)\mu(n)$. This is trivial for $m = n = 1$. Now if we choose either $p^2|n$ or $p^2|m$ then $p^2|mn$. Therefore $\mu(mn) = 0 = \mu(m)\mu(n)$. This case is also trivial. Now we assume m, n to be square-free integers. Then $m = p_1p_2\cdots p_a$, $n = q_1q_2\cdots q_b$ where p_i and q_j are all distinct, then $\mu(mn) = \mu(p_1p_2\cdots p_aq_1q_2\cdots q_b) = (-1)^{a+b} = (-1)^a(-1)^b = \mu(m)\mu(n)$. This proves that μ is a multiplicative function. □

Now from the above theorem we can see that both m and n are divisors of mn. A natural question arises how this function behaves with divisors of any integers. If $n = 1$ then the only divisor is $d = 1$ therefore $\sum_{d|1}\mu(d) = \mu(1) = 1$. So we have to discuss the divisors for those $n > 1$ and for that we need to apply the formula $F(n) = \sum_{d|n}\mu(d)$ which has already been discussed in the first section of this chapter. Our next theorem illustrates the clarification of this discussion.

Theorem 6.4.2. *For each positive integer*

$$n \geq 1, \ \sum_{d|n}\mu(d) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n > 1. \end{cases}$$

where d is positive divisors of n.

Proof. The assertion is obvious if $n = 1$, then $\sum_{d|n}\mu(d) = \mu(1) = 1$. We proceed by mathematical induction on the number of different prime factors of n when $n > 1$ and if $n = p^\alpha$, then

$$\sum_{d|p^\alpha}\mu(d) = \mu(1) + \mu(p) + \ldots + \mu(p^\alpha) = 1 + (-1) = 0.$$

Since μ is multiplicative, using Theorem 6.2.4, F is also so. Thus if

$$n = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_r^{\alpha_r},$$

then

$$\sum_{d|n}\mu(d) = \sum_{d|p_1^{\alpha_1}}\mu(d)\sum_{d|p_2^{\alpha_2}}\mu(d)\cdots\sum_{d|p_r^{\alpha_r}}\mu(d) = 0.$$

□

To illustrate the above theorem let us consider $n = 12$, the divisors of 12 are $1, 2, 4, 3, 6$ and 12. Thus the required sum is,

$$\begin{aligned}\sum_{d|12}\mu(d) &= \mu(1)+\mu(2)+\mu(3)+\mu(4)+\mu(6)+\mu(12)\\ &= 1+(-1)+(-1)+0+(-1)^2+0=0.\end{aligned}$$

In mathematics, the classic Mobi*üs* inversion formula was introduced into number theory on 1832 by August Ferdinand Mobi*üs*, stated as follows:

Theorem 6.4.3. *Mobiüs Inversion Formulae: Let* F *and* f *be two number theoretic functions related by the formulae* $F(n)=\sum_{d|n} f(d)$ *and,* $f(n)=\sum_{d|n}\mu(d)F(n/d)$ *for every* n*. If either of them is true then they satisfy both the formulae.*

Proof. Let us first choose that $F(n)=\sum_{d|n} f(d)$, then

$$\begin{aligned}\sum_{d|n}\mu(d)F(n|d) &= \sum_{dd'=n}\mu(d)F(d'), \quad \text{since integer } d' \text{ is the quotient when } d|n\\ &= \sum_{dd'=n}\mu(d)\sum_{e|d'} f(e), \quad \text{since } F(n)=\sum_{d|n} f(d) \text{ for each } n\\ &= \sum_{dek=n}\mu(d)f(e), \quad \text{as integer } k \text{ is the quotient when } e|d'\\ &= \sum_{ek'=n} f(e)\sum_{d|k'}\mu(d), \quad \text{taking integer } k'=dh \text{ for some integer } h.\end{aligned}$$

Now if $k'=1$, then using the Theorem 6.4.2 we have, $\sum_{d|k'}\mu(d)=1$. Therefore $\sum_{d|n}\mu(d)F(n|d)=f(n)$.

Conversely let, $f(n)=\sum_{d|n}\mu(d)F(n/d)$ holds. Then,

$$\begin{aligned}\sum_{d|n} f(d) &= \sum_{d|n}\left(\sum_{d'|d}\mu(d)F\left(\frac{d}{d'}\right)\right)\\ &= \sum_{d'pq=n}\mu(d')F(p), \quad \text{Since } d=d'p, n=qd=d'pq \text{ for some integer } p \text{ and } q\\ &= \sum_{ph'=n} F(p)\sum_{d'|h'}\mu(d') \quad \text{where, } h'=d'q \text{ for some integer } h'.\end{aligned}$$

Now again applying Theorem 6.4.2 we have,$\sum_{d'|h'}\mu(d')=1$ if $h'=1$ holds. Therefore $\sum_{d|n} f(d)=F(n)$. □

Before going to the last result of this section we see from Theorem 6.2.4 that if $f(n)$ is multiplicative then $F(n)$ is also multiplicative for each integer n. Now the question arises, is the converse assertion also true. The following theorem illustrates the answer of it.

Theorem 6.4.4. *If F is a multiplicative function and $F(n) = \sum_{s|n} f(s)$ then f is also multiplicative for any integer n and positive divisor s.*

Proof. Let m, n be relatively prime positive integers then any divisor s of mn can be uniquely written as $s = s_1 s_2$ where $s_1|m$ and $s_2|n$ where $\gcd(s_1, s_2) = 1$. Now by inversion formulae we have,

$$\begin{aligned} f(mn) = \sum_{s|mn} \mu(s) F\left(\frac{mn}{s}\right) &= \sum_{s_1|m, s_2|n} \mu(s_1 s_2) F\left(\frac{mn}{s_1 s_2}\right) \\ &= \left(\sum_{s_1|m} \mu(s_1) F\left(\frac{m}{s_1}\right)\right)\left(\sum_{s_2|n} \mu(s_2) F\left(\frac{n}{s_2}\right)\right) \\ &= f(m) f(n) \text{ (Why!)}. \end{aligned}$$

This proves the theorem. □

6.5 Worked out Exercises

Problem 6.5.1. *Suppose a function Λ is defined by*

$$\Lambda(n) = \begin{cases} \ln p, & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1; \\ 0, & \text{otherwise.} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = -\sum_{d/n} \mu(d) \ln d$.

Solution 6.5.1. *Let $n = p^k$. Then*

$$\sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = \mu(p^k) \ln 1 + \mu(p^{k-1}) \ln p + \ldots + \ldots + \mu(p^{k-i}) \ln p^i + \ldots + \mu(p^0) \ln p^k.$$

Case(i) *If $k = 1$, then $\sum_{d/n} \mu\left(\frac{n}{d}\right) \ln d = \ln p$ (Verify!).*

Case(ii) *If $k > 1$, then $\mu(p^{k-i}) = 0$ except for $i = 1, 2$. Then the sum is same as $k = 1$.*

Hence $\sum_{d/n}\mu\left(\frac{n}{d}\right)\ln d=\ln p=\Lambda(n)$. *Next*

$$\sum_{d/n}\mu(d)\ln d=\mu(p^0)\ln 1+\mu(p^1)\ln p^1+\ldots+\ldots+\mu(p^i)\ln p^i+\ldots+\mu(p^k)\ln p^k.$$

For $k>1,\ \mu(p^k)=0$ *implies* $\sum_{d/n}\mu(d)\ln d=-\ln p$ *for all* k. *Hence*

$$\sum_{d/n}\mu(d)\ln d=-\Lambda(n).$$

Remark 6.5.1. *The function* Λ *in the Problem 6.5.1 is known as Mangoldt function.*

Problem 6.5.2. *Let* $n=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$ *be the prime factorization of the integer* $n>1$. *If* f *is a multiplicative function that is not identically zero, prove that*

$$\sum_{d/n}\mu(d)f(d)=(1-f(p_1))(1-f(p_2))\cdots(1-f(p_s)).$$

Solution 6.5.2. *Since* μ *and* f *is multiplicative, therefore* μf *is also so(Why!). By virtue of Theorem 6.2.4,* $F(n)=\sum_{d/n}\mu(d)f(d)$ *is multiplicative. Consider,*

$$\begin{aligned}F(p^k)&=\sum_{d/p^k}\mu(d)f(d)\\&=\mu(1)f(1)+\mu(p)f(p)+\cdots+\mu(p^k)f(p^k)\\&=\mu(1)f(1)+\mu(p)f(p)(Why!)\\&=1f(1)+(-1)f(p)\\&=f(1)-f(p).\end{aligned}$$

Since for a multiplicative function not identically zero, therefore $f(1)=1$ *implies* $F(p^k)=1-f(p)$. *Thus*

$$\sum_{d/n}\mu(d)f(d)=(1-f(p_1))(1-f(p_2))\cdots(1-f(p_s)).$$

Problem 6.5.3. *Let* $S(n)$ *denote the number of square-free divisors of* n. *Prove that*

$$S(n)=\sum_{d/n}|\mu(d)|=2^{\omega(n)},$$

where $\omega(n)$ *is the number of distinct prime divisors of* n.

Solution 6.5.3. *Consider,*

$$|\mu(n)| = \begin{cases} 1, & \textit{if } n = 1; \\ 0, & \textit{if } p^2|n, \ p \textit{ being prime }; \\ 1, & \textit{if } n = p_1 p_2 \cdots p_s, \ p_i \textit{ being distinct.} \end{cases}$$

Let $\gcd(m,n) = 1$*. Then* $|\mu(1)| = 1$*. If* $m = 1$*, then* $|\mu(mn)| = |\mu(n)| = |\mu(m)||\mu(n)|$*. If* $p^2|m$*, then* $p^2|mn$ *implies* $|\mu(mn)| = 0$ *and* $|\mu(m)| = 0$*. Hence* $|\mu(mn)| = |\mu(m)\mu(n)|$*. Assume, both* m, n *are square-free. Let* $m = p_1 p_2 \cdots p_s$, $n = q_1 q_2 \cdots q_r$ *with* $p_i \neq q_j$ *as* $\gcd(m,n) = 1$*. Clearly,* $|\mu(m)| = |\mu(n)| = |\mu(mn)| = 1$*. Hence,* $|\mu(mn)| = |\mu(m)||\mu(n)|$*. This shows* $|\mu(n)|$ *is multiplicative. Using Theorem (6.2.4),* $S(n) = \sum_{d/n} |\mu(n)|$ *is also so.*

Now, consider $n = p^k$*. The divisors of* n *are* $1, p, p^2, \ldots, p^k$*. Therefore*

$$S(n) = \sum_{d/n} |\mu(n)| = 2.$$

The number of square-free divisors of p^k *is* 2 *and is defined by* $\sum_{d/n} |\mu(n)|$*. Given that,* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$*. From Theorem 6.2.1, all the square divisors of* n *are represented by* $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, $0 \leq a_j \leq 1$*. Here the number of square-free divisors of* p_i *is* 2*, which are* 1 *&* p_i*. It is true for all* $i = 1, 2, 3, \ldots, s$*. Hence the total number of square-free integers is* $2^s = 2^{\omega(n)}$*, where* $\omega(n)$ *is the number of distinct prime divisors of* n*. Therefore*

$$\begin{aligned} S(n) &= S(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \\ &= S(p_1^{k_1}) S(p_2^{k_2}) \cdots S(p_s^{k_s}) \\ &= \Bigg(\sum_{d/p_1^{k_1}} |\mu(p_1^{k_1})| \Bigg) \cdots \Bigg(\sum_{d/p_1^{k_1}} |\mu(p_s^{k_s})| \Bigg) \\ &= 2^s = 2^{\omega(n)}. \end{aligned}$$

Problem 6.5.4. *The Liouville* λ *function defined as*

$$\lambda(z) = \begin{cases} (-1)^{t_1 + t_2 + \ldots + t_s}, & \textit{if } z = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}, \ z > 1; \\ 1, & \textit{if } z = 1. \end{cases}$$

1. *Prove that* λ *is multiplicative.*

2. *For some positive integer* z*, prove that*

$$\sum_{d/z} \lambda(d) = \begin{cases} 1, & \textit{if } z = k^2 \textit{ for some integer } k; \\ 0, & \textit{Otherwise.} \end{cases}$$

Solution 6.5.4. 1. *Let us consider two positive integers* z *and* k *with* $\gcd(z,k) = 1$*, where* $z = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, $k = q_1^{v_1} q_2^{v_2} \cdots q_r^{v_r}$.

Now $zk = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s} q_1^{v_1} q_2^{v_2} \cdots q_r^{v_r}$, $p_i \neq q_j$. *Hence*

$$\begin{aligned} \lambda(zk) &= (-1)^{t_1+t_2+\ldots+t_s+v_1+v_2+\ldots+v_r} \\ &= (-1)^{t_1+t_2+\ldots+t_s} \cdot (-1)^{v_1+v_2+\ldots+v_r} \\ &= \lambda(z)\lambda(k). \end{aligned}$$

This shows that $\lambda(z)$ *is multiplicative function.*

2. *Let* $F(z) = \sum_{d/z} \lambda(d)$. *Then by Theorem 6.2.4,* F *is multiplicative. Let* $z = p^t$. *Then,*

$$\begin{aligned} F(z) &= \lambda(1) + \lambda(p) + \lambda(p^2) + \ldots + \lambda(p^t) \\ &= 1 + (-1) + (-1)^2 + (-1)^3 + \ldots + (-1)^{t-1} + (-1)^t. \end{aligned}$$

Now, two cases may arise:

Case(i) t *is even: Then* $z = p^{2\omega}$, $t = 2\omega$ *for some positive integer* ω. *Therefore, taking* $m = p^{\omega}$, *we obtain* $z = m^2$. *Also,* $F(z) = 1$.

Case(ii) t *is odd: Then we have* $F(z) = F(p^t) = 0$. *Let* $n = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$. *Since* F *is multiplicative, therefore* $F(n) = F(p_1^{t_1})F(p_2^{t_2}) \cdots F(p_s^{t_s})$. *If* $z = k^2$ *for some integer* k, *then all the* t_i*'s are even. So* $F(p_i^{t_i}) = 1$ *and consequently,* $F(z) = 1$. *Again, if any of the* t_i *is odd, then* $F(p_i^{t_i}) = 0$. *So* $F(z) = 0$.

Problem 6.5.5. *For every integer* $z \geq 3$, *prove that* $\sum_{t=1}^{z} \mu(t!) = 1$.

Solution 6.5.5. *Here* $\mu(4) = 0$*(Why!). If* $n \geq 4$, *then* $z!$ *would contain* 4 *as a factor. Since* μ *is multiplicative, therefore for* $z \geq 4$, $\mu(z!) = 0$. *So, only case need to consider is* $z = 3$. *Now* $\mu(1) = 1$, $\mu(2) = -1 = \mu(3)$ *implies* $\sum_{t=1}^{3} \mu(t!) = 1 + (-1) + 1 = 1$.

6.6 Greatest Integer Function

In this section we are going to discuss a special type of arithmetic function called greatest integer function. The domain of definition of this function is the set of real numbers and the range set is the set of integers. This function is very much useful for calculating continued fractions. The definition of the function as follows.

Definition 6.6.1. *For an arbitrary real number* x, *the largest integer less than or equal to* x *and denoted by* $[x]$ *is called the greatest integer function.*

For an example we have $[2.2] = 2$ and $[-2.2] = -3$. Here for every real number x, there is a unique real number θ such that $x = [x] + \theta, 0 \leq \theta < 1$, where θ is the fractional part of x. This θ sometimes denoted as $\{x\}$ such that $x = [x]+\{x\}, \forall x \in \mathbb{R}$. Actually the greatest integer function for any real number x follows the inequality $x - 1 < [x] \leq x$. In our next proposition we have shown division algorithm using this inequality.

Proposition 6.6.1. *For any $x \in \mathbb{R}$, prove division algorithm by the inequality $x - 1 < [x] \leq x$.*

Proof. Let $q = \left[\frac{m}{n}\right]$ and $r = m - n\left[\frac{m}{n}\right]$, clearly $m = nq + r$ and we will show that the remainder satisfies the above inequality. As $\dfrac{m}{n} \in \mathbb{R}$ then $\left(\frac{m}{n}\right) - 1 < \left[\frac{m}{n}\right] \leq \frac{m}{n}$. Now multiplying by $-n$ the above inequality and changing the order of inequality we have, $-m \leq -n\left[\frac{m}{n}\right] < n - m$. Adding m we get, $0 \leq m - n\left[\frac{m}{n}\right] < n \Rightarrow 0 \leq r < n$. We are to show this q and r are unique. Let us assume that they are not unique then $m = nq_1 + r_1 = nq_2 + r_2$ for q_1, q_2 are quotients and $0 \leq r_1, r_2 < n$ where r_1, r_2 are remainders. Now subtracting these two equations we have, $0 = n(q_1 - q_2) + (r_1 - r_2)$ thus $(r_2 - r_1) = n((q_1 - q_2))$ which implies $n|(r_1 - r_2)$ but this is possible only if $r_1 - r_2 = 0$. Therefore $r_1 = r_2$ and $q_1 - q_2$, which shows that q is unique quotient and r is unique remainder. ☐

Now we will discuss few properties related to this greatest integer function.

Proposition 6.6.2. *For any $x, y \in \mathbb{R}$ and $m \in \mathbb{Z}$, the greatest integer function satisfies following properties:*

(i) $[x + m] = [x] + m$

(ii) $[x] + [-x] = \begin{cases} 0, & \text{if } x \in \mathbb{Z}; \\ -1, & \text{if } x \in \mathbb{R} \setminus \mathbb{Z}. \end{cases}$

(iii) $[x] + [y] \leq [x + y]$

(iv) $\left[\dfrac{x}{m}\right] = \left[\dfrac{[x]}{m}\right]$.

Proof. Let $x = n + \theta$ for $n \in \mathbb{Z}, 0 \leq \theta < 1$,

(i) Here, $x + m = (n + m) + \theta$ where $m + n \in \mathbb{Z},\ 0 \leq \theta < 1$. Thus

$$[x + m] = n + m = [x] + m.$$

(ii) Here,

$$-x = \begin{cases} -n - \theta, & 0 \geq -\theta > -1; \\ (-n - 1) + (1 - \theta), & 0 < 1 - \theta \leq 1. \end{cases}$$

Therefore

$$[-x] = \begin{cases} -(1+n), & \text{if } 1-\theta \neq 1; \\ -n, & \text{if } 1-\theta = 1. \end{cases}$$

This proves that

$$[x] + [-x] = \begin{cases} -1, & \text{if } x \notin \mathbb{Z}; \\ 0, & \text{if } x \in \mathbb{Z}. \end{cases}$$

(iii) Let $y = r + \theta'$, $r \in \mathbb{Z}$, $0 \leq \theta' < 1$. Therefore

$$x + y = (n + r) + (\theta + \theta'), 0 \leq (\theta + \theta') < 2.$$

Thus we have,

$$[x+y] = \begin{cases} n+r, & \text{if } 0 \leq \theta + \theta' < 1; \\ n+r+1, & \text{if } \theta + \theta' \geq 1. \end{cases}$$

Hence

$$[x] + [y] = n + r \leq [x + y].$$

(iv) Now let $\dfrac{x}{m} = z + \widetilde{\theta}$, $z \in \mathbb{Z}$ and $0 \leq \widetilde{\theta} < 1$. Then we have

$$x = mz + m\widetilde{\theta},\ mz \in \mathbb{Z} \text{ and } 0 \leq m\widetilde{\theta} < m.$$

Therefore

$$\left[\frac{[x]}{m}\right] = [z] = z \text{ as } x \in \mathbb{Z}.$$

Hence

$$\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right].$$

□

Now we are going to the application part of this greatest integer function. For that we choose an integer 7 whose factorial is $7! = 1{\cdot}2{\cdot}3{\cdot}4{\cdot}5{\cdot}6{\cdot}7 = 2^4{\cdot}3^2{\cdot}5{\cdot}7$. Here we can see that the highest power of 2 which divides 7! is 4. We can find the exponent of any prime which occurs in prime factorization of any factorial of an integer by greatest integer function using the next theorem.

Theorem 6.6.1. *If p is a prime then, $\displaystyle\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$ is the exponent of p appearing in the prime factorization of $n!$.*

Proof. If $p > n$ then p does not appear in the prime factorization of $n!$. Thus we have $p \leq n$. Among the first n positive integers those who are divisible by p are $p, 2p, 3p \cdots \left[\frac{n}{p}\right]p$. Thus there exists exactly $\left[\frac{n}{p}\right]$ multiples of p occuring in the product of $n!$. Among those integers $p, 2p, 3p \cdots \left[\frac{n}{p}\right]p$ there are $\left[\frac{n}{p^2}\right]$ integers which are again divisible by p^2 and they are $p^2, 2p^2, 3p^2 \cdots \left[\frac{n}{p^2}\right]p^2$. After continuing these steps finitely many times we get the total number of times p divides $n!$ is $\displaystyle\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$. □

Now we will illustrate this theorem by means of an example.

Example 6.6.1. *Let us take* $n = 10$ *and* $p = 2$ *then there are* $\left[\frac{10}{2}\right] = 5$ *integers which are divisible by* $p = 2$ *and they are* $2, 4, 6, 8, 10$. *Among those integers there are* $\left[\frac{10}{2^2}\right] = 2$ *integers which are divisible by* 4 *and they are* $4, 8$. *Now among these two integers there are* $\left[\frac{10}{2^3}\right] = 1$ *integers which are divisible by* 8 *and it is* 8 *itself.Therefore the total number is* $\left[\frac{10}{2}\right]+\left[\frac{10}{2^2}\right]+\left[\frac{10}{2^3}\right] = 8$.*Now* $10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$. *So the highest power of* 2 *is* 8.

In our next two results we are going to find some common well known facts of mathematics by using the last theorem.

Theorem 6.6.2. *If* n *and* r *are positive integers with* $1 \leq r < n$, *then the binomial coefficient* $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ *is an integer.*

Proof. For proving $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ is an integer we are only to show $n!$ is divisible by $r!(n-r)!$. Now from the Theorem 6.6.1 we have the exponent of highest power of prime p that divides $n!$ is $\displaystyle\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$ and the highest power of prime p that divides $\frac{n!}{r!(n-r)!}$ is $\displaystyle\sum_{i=1}^{\infty}\left[\frac{r}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{(n-r)}{p^i}\right]$. Again from the Proposition 6.6.2(iii) we have $[a+b] \geq [a] + [b]$ for any two integers a, b. Then we have,

$$\left[\frac{n}{p^i}\right] \geq \left[\frac{r}{p^i}\right] + \left[\frac{(n-r)}{p^i}\right].$$

Taking the summation we get,

$$\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right] \geq \sum_{i=1}^{\infty}\left[\frac{r}{p^i}\right] + \sum_{i=1}^{\infty}\left[\frac{(n-r)}{p^i}\right].$$

From the above inequality it follows that p occurs in the numerator of $\dfrac{n!}{r!(n-r)!}$ at least as many times in the denominator. As p is arbitrary so $r!(n-r)!$ must divide $n!$. Thus $\dfrac{n!}{r!(n-r)!}$ is an integer. $\square$

Corollary 6.6.1. *For any positive integer r, the product of r consecutive integers is divisible by $r!$.*

Proof. Here we can assume the product of r consecutive integers as $n(n-1)\cdots(n-r+1)$ where n is largest. Here $n(n-1)\cdots(n-r+1) = \dfrac{n!}{r!(n-r)!} = \left(\dfrac{n!}{r!(n-r)!}\right) \times r!$ and from the Theorem 6.6.2 we know that $\dfrac{n!}{r!(n-r)!}$ is an integer.This proves the assertion of this corollary. $\square$

In our later part of discussion on greatest integer function we have shown some valuable relations between this function and other arithmetic functions. Their relationship comes out as,

Theorem 6.6.3. *Let f and F be two arithmetic functions such that $F(n) = \sum_{d|n} f(d)$ where n is a positive integer. Then for any positive integer N, $\sum_{n=1}^{N} F(n) = \sum_{m=1}^{N} f(m)\left[\dfrac{N}{m}\right]$.*

Proof. We are going to start the theorem by the form of $F(n)$. Taking the sum over this function we have $\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N}\sum_{d|n} f(d)$. Here we are to collect the terms with equal values of $f(d)$. Since each integer divides itself then the assertion for a fixed positive integer $m \leq N$, the term $f(m)$ appears in $\sum_{d|n} f(d)$ if and only if m is a divisor of n is possible. Now to calculate the number of terms in the sum $\sum_{d|n} f(d)$ in which $f(m)$ occurs as a term, it is sufficient to find the number of integers from the set $\{1, 2, \cdots N\}$ which are divisible by m.From the Theorem 6.6.1 there are exactly $\left[\dfrac{N}{n}\right]$ of them. Thus for each m such that $1 \leq m \leq N$, $f(m)$ is a term of the sum $\sum_{d|n} f(d)$ for $\left[\dfrac{N}{n}\right]$ different positive integers less than or equal to N. Therefore

$$\sum_{n=1}^{N}\sum_{d|n} f(d) = \sum_{m=1}^{N} f(m)\left[\frac{N}{m}\right] = \sum_{n=1}^{N} F(n)$$

This proves the theorem. □

Our next corollary is the immediate application of this theorem on two arithmetic functions $\tau(n)$ and $\sigma(n)$.

Corollary 6.6.2. *If N is a positive integer then,*

$$\sum_{n=1}^{N}\tau(n)=\sum_{n=1}^{N}\left[\frac{N}{n}\right] \text{ and } \sum_{n=1}^{N}\sigma(n)=\sum_{n=1}^{N}\left(n\left[\frac{N}{n}\right]\right).$$

Proof. We know that $\tau(n)=\sum_{d|n}1$ and $\sigma(n)=\sum_{d|n}d$. Now taking $F(n)=\tau(n)$ and $f(n)=1$, for all $n\in\mathbb{N}$ we have from the Theorem 6.6.3 $\sum_{n=1}^{N}\tau(n)=\sum_{n=1}^{N}\left[\frac{N}{n}\right]$. Again taking $F(n)=\sigma(n)$ and $f(n)=n$, for all $n\in\mathbb{N}$ we have from the Theorem 6.6.3 $\sum_{n=1}^{N}\sigma(n)=\sum_{n=1}^{N}\left(n\left[\frac{N}{n}\right]\right)$. □

Now to visualize those two forms of $\tau(n)$ and $\sigma(n)$ we will go through an example given below.

Exercise 6.6.1. *Let us consider $N=4$ then, $\sum_{n=1}^{4}\tau(n)=\tau(1)+\tau(2)+\tau(3)+\tau(4)=1+2+2+3=8$. Now,*

$$\sum_{n=1}^{4}\left[\frac{4}{n}\right]=[4]+[2]+\left[\frac{4}{3}\right]+[1]=4+2+1+1=8.$$

Also,

$$\sum_{n=1}^{4}\sigma(n)=\sigma(1)+\sigma(2)+\sigma(3)+\sigma(4)=1+3+4+7=15$$

and

$$\sum_{n=1}^{4}\left(n\left[\frac{4}{n}\right]\right)=1[4]+2[2]+3\left[\frac{4}{3}\right]+4[1]=4+4+3+4=15.$$

6.7 Worked out Exercises

Problem 6.7.1. *Find the highest power of* 5 *dividing* 1000!.

Solution 6.7.1.

$$\left[\frac{1000}{5}\right]+\left[\frac{1000}{5^2}\right]+\left[\frac{1000}{5^3}\right]+\left[\frac{1000}{5^4}\right]=249\Rightarrow 5^{249}|1000!.$$

Problem 6.7.2. *For an integer $z \geq 0$, show that* $\left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] = z.$

Solution 6.7.2. *By definition, we have the following inequalities:*

$$\frac{z}{2} - 1 < \left[\frac{z}{2}\right] \leq \frac{z}{2} \tag{6.7.1}$$

$$-\frac{z}{2} - 1 < \left[-\frac{z}{2}\right] \leq -\frac{z}{2}. \tag{6.7.2}$$

From equation (6.7.2), we have $-\left[-\frac{z}{2}\right] < \frac{z}{2} + 1$*. Adding the last inequation with (6.7.1), we obtain*

$$\left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] < \frac{z}{2} + \frac{z}{2} + 1 = z + 1 \leq z. \tag{6.7.3}$$

Further, from inequation (6.7.2), we have $\frac{z}{2} \leq -\left[-\frac{z}{2}\right]$*. Adding the foregoing inequation with (6.7.1), we obtain*

$$z \leq \left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] \text{ (How!)}. \tag{6.7.4}$$

Finally, (6.7.3) and (6.7.4) gives $\left[\frac{z}{2}\right] - \left[-\frac{z}{2}\right] = z.$

Problem 6.7.3. *If $z \geq 1$ and q is a prime, then find the exponent of the highest power of q that divides* $\frac{(2z)!}{(z!)^2}$*.*

Solution 6.7.3. *For any prime q, let s be the highest power of q that divides $(2z)!$. If $q|z!$, let k be the highest power of q such that $q^k|z!$. Thus $\frac{q^s}{q^k} = q^{s-k}$. So $s-k$ is the highest power of q satisfying $q^{s-k}\big|\frac{(2z)!}{(z!)}$. Also, $s-2k$ is the highest power of q satisfying $q^{s-k}\big|\frac{(2z)!}{(z!)^2}$. By virtue of Theorem 6.6.1, the highest power of q dividing $(2z)!$ is $\sum_{k=1}^{\infty}\left[\frac{2z}{q^k}\right]$ and the highest power of q dividing $z!$ is $\sum_{k=1}^{\infty}\left[\frac{z}{q^k}\right]$. Finally, the highest power of q dividing $\frac{(2z)!}{(z!)^2}$ is given by,*

$$\sum_{k=1}^{\infty}\left[\frac{2z}{q^k}\right] - 2\sum_{k=1}^{\infty}\left[\frac{z}{q^k}\right] = \sum_{k=1}^{\infty}\left(\left[\frac{2z}{q^k}\right] - 2\left[\frac{z}{q^k}\right]\right).$$

Problem 6.7.4. *Let the positive integer z be written in terms of powers of the prime q so that we have $z = a_k q^k + \ldots + a_2 q^2 + a_1 q + a_0$, where $0 \leq a_i < q$. Find the exponent of the highest power of q appearing in the prime factorization of $z!$.*

Solution 6.7.4. *Before finding the exponent of the highest power of q, let us state and prove the following lemma viz*

Lemma 6.7.1. *For* $q > 1, z > 1$; $\quad (q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^z}\right) < 1.$

Proof. By principle of mathematical induction we are going to prove the above lemma. For $k = 1$, the lemma is trivial(Verify!). Suppose the lemma is true for $z = k$. Then

$$(q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^k}\right) < 1.$$

Therefore

$$\begin{aligned}(q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^k} + \frac{1}{q^{k+1}}\right) &= (q-1)\left(\frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{q^k}\right) + \frac{q-1}{q^{k+1}} \\ &= q\left(\frac{1}{q} + \ldots + \frac{1}{q^k}\right) - \frac{1}{q} - \ldots - \frac{1}{q^k} + \frac{1}{q^k} - \frac{1}{q^{k+1}}.\end{aligned}$$

By hypothesis $q\left(\frac{1}{q} + \ldots + \frac{1}{q^k}\right) - \frac{1}{q} - \ldots - \frac{1}{q^k} < 1$, therefore

$$\begin{aligned}q\left(\frac{1}{q} + \ldots + \frac{1}{q^k}\right) - \frac{1}{q} - \ldots - \frac{1}{q^k} + \frac{1}{q^k} - \frac{1}{q^{k+1}} &< 1 + \frac{1}{q^k} - \frac{1}{q^{k+1}} \\ &< 1 - \frac{1}{q^{k+1}} \\ &< 1.\end{aligned}$$

Hence the lemma is true for $z = k + 1$.

Using Theorem 6.6.1 the exponent of the highest power of q appearing in the prime factorization of $z!$ is

$$\begin{aligned}\sum_{i=1}^{\infty}\left[\frac{z}{q^i}\right] = &\left[a_k q^{k-1} + \ldots + a_2 q + a_1 + \frac{a_0}{q}\right] \\ &+ \left[a_k q^{k-2} + \ldots + a_2 + \frac{a_1}{q} + \frac{a_0}{q^2}\right] \\ &+ \\ &\vdots \\ &+ \\ &+ \left[a_k + \ldots + \ldots + \frac{a_1}{q^{k-1}} + \frac{a_0}{q^k}\right] \\ &+ \left[\frac{a_k}{q} + \ldots + \ldots + \frac{a_1}{q^k} + \frac{a_0}{q^{k+1}}\right].\end{aligned} \tag{6.7.5}$$

In equation (6.7.5), all $0 \leq a_i \leq q-1$. Note that $\left[\frac{z}{q^k}\right] q = a_k q = \left[\frac{z}{q^{k-1}}\right] - a_{k-1}$.

Therefore

$$\begin{aligned}\left[\frac{z}{q^1}\right] q &= z - a_0\\ \left[\frac{z}{q^2}\right] q &= \left[\frac{z}{q}\right] - a_1\\ &\vdots\\ \left[\frac{z}{q^{k-1}}\right] q &= \left[\frac{z}{q^{k-2}}\right] - a_{k-2}\\ \left[\frac{z}{q^{k}}\right] q &= \left[\frac{z}{q^{k-1}}\right] - a_{k-1}\\ 0 &= \left[\frac{z}{q^{k}}\right] - a_k.\end{aligned}$$

On adding the left and right column entries, we have

$$\left(\left[\frac{z}{q^1}\right] + \left[\frac{z}{q^2}\right] + \ldots + \left[\frac{z}{q^{k-1}}\right] + \left[\frac{z}{q^k}\right]\right)(q-1) = z - (a_0 + a_1 + \ldots + a_k).$$

Hence

$$\sum_{k=1}^{\infty} \left[\frac{z}{q^k}\right] = \frac{z - (a_0 + a_1 + \ldots + a_k)}{q-1}.$$

Problem 6.7.5. *Using Problem 6.7.4, find the exponent of highest power of* p *dividing* $(p^k - 1)!$.

Solution 6.7.5. *Hint: Here,*

$$\begin{aligned}p^k - 1 &= (p-1)(p^{k-1} + p^{k-2} + \ldots + p + 1)\\ &= (p-1)p^{k-1} + (p-1)p^{k-2} + \ldots + (p-1)p + (p-1).\end{aligned}$$

Since, p *is prime,* $0 \le p - 1 \le p$ *so*

$$a_{k-1} = p-1,\ a_{k-2} = p-1, \ldots,\ a_1 = p-1,\ a_0 = p-1.$$

Take $z = p^k - 1$ *and apply the formulae in Problem 6.7.4.*

Problem 6.7.6. *For any positive integer* N*, verify the formulae:*

$$\sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right] = [\sqrt{N}].$$

Solution 6.7.6. *Let* $F(z) = \sum_{d|z} \lambda(d)$*,* λ *being the Liouville function defined in Problem 6.5.4. Taking help of Theorem 6.6.3, we have* $\sum_{z=1}^{N} F(z) = \sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right]$.

Moreover, by Problem (6.5.4) we have

$$F(z) = \begin{cases} 1, & \textit{if } z = m^2 \textit{ for some integer } m; \\ 0, & \textit{Otherwise.} \end{cases}$$

Therefore $\sum_{z=1}^{N} F(z)$ *monitor the number of perfect squares less than or equal to* N *as* F *assigns a value of* 1 *to each* z *that can be expressed as a perfect square. Thus*

$$\sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right] = \textit{Number of squares} \leq N.$$

Next let us consider, $[\sqrt{N}]$ *and perfect squares, which are* $1^2, 2^2, 3^2$*, and so on. For any* $N = m^2$*, there are exactly* m *perfect squares(positive integers) less than or equal to* N*. Suppose* $[\sqrt{N}]$ *is not an integer* m *be the largest integer satisfying* $m^2 < N$*. Therefore* $N < (m+1)^2 \Rightarrow m < \sqrt{N} < m+1$*. Since* $m = \sqrt{N}$*, therefore* $\sqrt{N}$ *is the number of perfect squares less than or equal to* N*. Hence* $\sum_{z=1}^{N} \lambda(z) \left[\frac{N}{z}\right] = [\sqrt{N}]$*.*

Problem 6.7.7. *If* N *is a positive integer, prove that*

$$\tau(N) = \sum_{z=1}^{N} \left(\left[\frac{N}{z}\right] - \left[\frac{N-1}{z}\right] \right).$$

Solution 6.7.7. *Applying Corollary 6.6.2, yields* $\sum_{z=1}^{N} \left[\frac{N}{z}\right] = \sum_{z=1}^{N} \tau(z)$*. Therefore*

$$\begin{aligned} \sum_{z=1}^{N} \left[\frac{N-1}{z}\right] &= \sum_{z=1}^{N-1} \left[\frac{N-1}{z}\right] + \left[\frac{N-1}{N}\right] \\ &= \sum_{z=1}^{N-1} \tau(z) + \left[\frac{N-1}{N}\right]. \end{aligned}$$

As $\frac{N-1}{z} < 1 (\forall N > 0)$*, therefore* $\left[\frac{N-1}{N}\right] = 0$*. Hence* $\sum_{z=1}^{N} \left[\frac{N-1}{z}\right] = \sum_{z=1}^{N-1} \tau(z)$*. Therefore* $\sum_{z=1}^{N} \left(\left[\frac{N}{z}\right] - \left[\frac{N-1}{z}\right] \right) = \sum_{z=1}^{N} \tau(z) - \sum_{z=1}^{N-1} \tau(z) = \tau(N)$*.*

Problem 6.7.8. *Given a positive integer* N*, prove:* $\sum_{z=1}^{N} \mu(z) \left[\frac{N}{z}\right] = 1$*.*

Solution 6.7.8. *Let* $F(z) = \sum_{d|z} \mu(d)$*. By Theorem 6.4.2, we find*

$$F(z) = \begin{cases} 1, & \textit{if } z = 1; \\ 0, & \textit{if } z > 1. \end{cases}$$

By Theorem 6.6.1, we have

$$\begin{aligned}\sum_{k=1}^{N} F(k) &= \sum_{z=1}^{N} \mu(z)\left[\frac{N}{z}\right] \\ &= F(1)+F(2)+\ldots+F(N) \\ &= 1.\end{aligned}$$

Hence $\sum_{z=1}^{N} \mu(z)\left[\frac{N}{z}\right] = 1$.

Let us illustrate the problem taking $N = 6$.

$$\begin{aligned}\sum_{z=1}^{6} \mu(z)\left[\frac{6}{z}\right] &= \mu(1)\left[\frac{6}{1}\right]+\mu(2)\left[\frac{6}{2}\right]+\mu(3)\left[\frac{6}{3}\right]+\mu(4)\left[\frac{6}{4}\right]+\mu(5)\left[\frac{6}{5}\right]+\mu(6)\left[\frac{6}{6}\right] \\ &= 1\cdot 6+(-1)\cdot 3+(-1)\cdot 2+0\cdot 1+(-1)\cdot 1+1\cdot 1 \\ &= 6-3-2+0-1+1 \\ &= 1.\end{aligned}$$

Problem 6.7.9. *Given a positive integer* N, *prove:* $\left|\sum_{z=1}^{N} \frac{\mu(z)}{z}\right| \leq 1$.

Solution 6.7.9. *From Problem 6.7.8, we obtain*

$$\sum_{z=1}^{N} \mu(z)\left[\frac{N}{z}\right] = 1 \Rightarrow \sum_{z=1}^{N-1} \mu(z)\left[\frac{N}{z}\right] + \mu(N) = 1.$$

Dividing by N, *we obtain from foregoing equation*

$$\frac{\mu(N)}{N} = \frac{1}{N} - \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\left[\frac{N}{z}\right]. \qquad (6.7.6)$$

Again,

$$\begin{aligned}\sum_{z=1}^{N} \frac{\mu(z)}{z} &= \sum_{z=1}^{N-1} \frac{\mu(z)}{z} + \frac{\mu(N)}{N} \\ &= \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\frac{N}{z} + \frac{\mu(N)}{N}. \qquad (6.7.7)\end{aligned}$$

(6.7.6) and (6.7.7) yields

$$\begin{aligned}\sum_{z=1}^{N} \frac{\mu(z)}{z} &= \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\frac{N}{z} + \frac{1}{N} - \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\left[\frac{N}{z}\right] \\ &= \frac{1}{N}\sum_{z=1}^{N-1} \mu(z)\left(\frac{N}{z} - \left[\frac{N}{z}\right]\right) + \frac{1}{N}.\end{aligned}$$

Since

$$|a+b| \leq |a|+|b|,\ |a\cdot b| = |a|\cdot|b|,\ 0 \leq \left|\frac{N}{z}-\left[\frac{N}{z}\right]\right| < 1 \ \mathit{and} \ \left|\frac{1}{N}\right| = \frac{1}{N},$$

therefore

$$\begin{aligned}\left|\sum_{z=1}^{N}\frac{\mu(z)}{z}\right| &\leq \frac{1}{N}\sum_{z=1}^{N-1}|\mu(z)|\left|\frac{N}{z}-\left[\frac{N}{z}\right]\right| + \frac{1}{N}\\ &\leq \frac{1}{N}\sum_{z=1}^{N-1}|\mu(z)| + \frac{1}{N}\\ &\leq \frac{1}{N}(N-1)+\frac{1}{N} = 1 \ \mathit{as}\ |\mu(z)| \leq 1.\end{aligned}$$

Let us illustrate the problem taking $N = 6$.

$$\begin{aligned}\left|\sum_{z=1}^{6}\frac{\mu(z)}{z}\right| &= \frac{\mu(1)}{1}+\frac{\mu(2)}{2}+\frac{\mu(3)}{3}+\frac{\mu(4)}{4}+\frac{\mu(5)}{5}+\frac{\mu(6)}{6}\\ &= \left|1+\left(-\frac{1}{2}\right)+\left(-\frac{1}{3}\right)+\frac{0}{4}+\left(-\frac{1}{5}\right)+\frac{1}{6}\right|\\ &= \left|1+\left(-\frac{5}{6}\right)+\left(-\frac{1}{5}\right)+\frac{1}{6}\right|\\ &= \left|1+\left(-\frac{13}{15}\right)\right| = \frac{2}{15} < 1.\end{aligned}$$

6.8 Exercises:

1. Show that $\sigma(n) = \sigma(n+1)$ for $n = 14, 206, 957$.
2. For any positive integer n, prove that $\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \ldots + \frac{1}{n}$.
3. Given a positive integer $k > 1$, show that there are infinitely many integers n for which $\tau(n) = k$, but at most finitely many n with $\sigma(n) = k$.
4. Prove that there are no positive integers n satisfying $\sigma(n) = 10$.
5. Show that for $k \geq 2$, if $2^k - 3$ is prime, then $n = 2^{k-1}(2^k - 3)$ satisfies the equation $\sigma(n) = 2n + 2$.
6. Prove that if f and g are multiplicative functions, then so is their product fg and quotient $\frac{f}{g}$(whenever the latter function is defined).
7. For any positive integer n, show that

$$\sum_{d|z}\frac{z}{d}\sigma(d) = \sum_{d|z} d\tau(d).$$

8. Given $z \geq 1$, let $\sigma_s(z)$ denote the sum of the sth powers of the positive divisors of z; that is, $\sigma_s(z) = \sum\limits_{d|z} d^s$. Prove that σ_s is a multiplicative function.

9. For each positive integer n, verify that $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

10. If the integer $n > 1$ has a prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, prove the following
    (a) $\sum_{d|n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \dots p_r$;
    (b) $\sum_{d|n} \frac{\mu(d)}{d} = (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$.

11. If the integer $n > 1$ has a prime factorization $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, then establish that $\sum_{d|n} \mu(d)\lambda(d) = 2^r$.

12. Find the highest power of 7 dividing 2000!.

13. If $n \geq 1$ and p is a prime, show that $\frac{(2n)!}{(n!)^2}$ is an even integer.

14. Find an integer $n \geq 1$ such that the highest power of 5 contained in $n!$ is 100.

15. Determine the highest power of 3 dividing 80! and the highest power of 7 dividing 2400!.

7

Euler's Generalization and ϕ–function

> *"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reasons to believe that it is a mystery into which the human mind will never penetrate."*
>
> – Leonhard Euler

7.1 Introduction

Fermat's work does not contribute much to the mathematics of his own day but creates a lasting impression on later generations of mathematics and Leonhard Euler (1707 – 1783) was the first one to appreciate its significance. Many theorems(without proof) were proclaimed by Fermat, and were later on proved by Euler with the similar arguments formulated by him.

Present chapter deals with Euler's generalization of Fermat's Little Theorem, depending on a function which indeed was invented by Euler, but named by J. J. Sylvester(1814 – 1897) in 1883. Euler's generalisations concerns congruences with prime moduli to arbitrary moduli.

Euler's theorem has great contributions in Economics. When $F(L, K)$ is a production function then Euler's theorem says that if factors of production are paid according to their marginal productivities, the total factor payment is equal to the degree of homogeneity of the production function times output.

Euler has great contribution in other fields of science such as function theory and theory of music, as well as the relationship between music and mathematics.

We give an account of the most important results obtained by Euler in number theory.

7.2 Euler's ϕ–function

The chapter, Fermat's little theorem addresses the congruence relation with a prime number. Now the question arises: Can we change the prime number by an arbitrary positive integer? The answer is in an affirmative sense and Euler's generalization is the important result which leads to that answer. Before going to this significant result we need to introduce an important arithmetic function called Euler's ϕ–function or Euler's totient function. To meet the purpose, first let us define this special type of function.

Definition 7.2.1. *For any positive integer n with $n \geq 1$, Euler's phi functionor Euler's totient function denoted as $\phi(n)$ and defined as the number of positive integers not exceeding n and relatively prime to n.*

Let us illustrate the above definition by some example, for which we displayed below a table of positive integers n and corresponding $\phi(n)$.

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

From the above table, it is clear that $\phi(1) = 1$ and $\phi(p) = p - 1$ for any prime p. Also, the converse with respect to second equality is true, *i.e.* if for any positive integer n, $\phi(n) = n - 1$ holds then n is prime. Our next proposition directs us to ensure the proof of this statement.

Proposition 7.2.1. *If p is a prime then $\phi(p) = p - 1$ holds and vice versa.*

Proof. If p is a prime, from the definition of ϕ-function, the number of integers which are less than p and prime to p is $p - 1$. Thus, $\phi(p) = p - 1$ for every prime p.

Conversely, let p be composite. Then it has a divisor q with $1 < q < p$ and $\gcd(p, q) \neq 1$. Now q belongs to the set $\{1, 2, 3, \cdots p - 1\}$ and q not relatively prime to p implies $\phi(p) \leq p - 2$. Hence if $\phi(p) = p - 1$ then p must be prime. □

The first important agenda of this section is, for any arbitrary positive integer n what should be $\phi(n)$ when the prime factorisation of n is known. The next few results of this section helps us to reach that platform from where we can find $\phi(n)$ for any arbitrary positive integer n.

Theorem 7.2.1. *If p is prime and $\alpha > 0$, then $\phi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$.*

Proof. Here we need to find those positive integers for which $\gcd(n, p^\alpha) = 1$ that is $p \nmid n$. Now given below the arrangement of those positive integers not greater than p^α. The arrangement is a rectangular array containing p columns and $p^{\alpha-1}$ rows:

$$\begin{array}{cccc} 1 & 2 & \cdots & p \\ p+1 & p+2 & \cdots & 2p \\ \vdots & \vdots & \vdots & \vdots \\ p^\alpha - p + 1 & p^\alpha - p + 2 & \cdots & p^\alpha \end{array}$$

and there are $p^{\alpha-1}$ integers between 1 and p^α which are divisible by p, namely

$$p, 2p, 3p, \ldots, p^{\alpha-1}.$$

p lies in rightmost column of the above array. Thus there are exactly $p^\alpha - p^{\alpha-1}$ integers which are relatively prime to p^α and so by definition of the ϕ–function, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$. □

To understand the above theorem lucidly by means of an example, let us choose $p = 2$ and $\alpha = 3$. Now using the table we have:

$$\begin{array}{cc} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{array}$$

Only the elements of the right sided column divides 2^3. Thus $\phi(2^3) = \phi(8)$ is the number of elements of the set $\{1, 3, 5, 7\}$ which is $4 = 2^{3-1}(2-1)$. We are now in the stage to find the phi function for prime powers. But still a question arises, whether it is possible to find the phi function of any positive integer directly whose prime factorization is given using the above theorem. The answer of this statement is in the affirmative sense but for that we have to check the multiplicative property of this arithmetic function ϕ. The next part of the present section deals with this fact.

Now we are in the position to state and prove the following theorem.

Theorem 7.2.2. *The function ϕ is a multiplicative function.*

Proof. It suffices to show that $\phi(mn) = \phi(m)\phi(n)$, where $\gcd(m, n) = 1$. If any one of m, n is 1, the result is true(Why!). Thus we may assume $m > 1, n > 1$. We arrange the integers from 1 to mn into $m \times n$ order array as follows:

$$\begin{array}{cccccc}
1 & 2 & \cdots & r & \cdots & m \\
m+1 & m+2 & \cdots & m+r & \cdots & 2m \\
2m+1 & 2m+2 & \cdots & 2m+r & \cdots & 3m \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & mn
\end{array}$$

We know that there are $\phi(mn)$ entries of the above array which are prime to mn(Why!) and this is same as the number of integers relatively prime to both m and n(refer to problem(2.6.1)). Now $\gcd(qm+r, m) = \gcd(r, m)$, so the numbers in $r-$th column are relatively prime to m if and only if $\gcd(r, m) = 1$. Thus there are only $\phi(m)$ columns containing integers relatively prime to m. Here every entry of that $\phi(m)$ columns are relatively prime to m. Now to show each of these $\phi(m)$ columns there are $\phi(n)$ integers which are relatively prime to n. In the entries of r-th column there are n integers $r, m+r, \ldots, (n-1)m+r$ no two of which are congruent modulo n. If it happens, let $(im+r) \equiv (jm+r)(\bmod n)(0 \leq i < j < n)$. Therefore $im \equiv jm(\bmod n)$ implies $i \equiv j(\bmod n)$ as $\gcd(m, n) = 1$, which leads to a contradiction. Thus the numbers in the r-th column are congruent modulo n to $0, 1, 2, \cdots, n-1$, in some order. If $s \equiv t(\bmod n)$ for some integer s and t then $\gcd(s, n) = 1$ if and only if $\gcd(t, n) = 1$. Thus r-th column contains as many integers, which are relatively prime to n, as does the set $\{0, 1, 2, \ldots, n-1\}$, namely $\phi(n)$. Therefore the total number of entries in the array that are relatively prime to both m, n is $\phi(m)\phi(n)$. $\square$

Finally, we are in the position to find the phi-function for any arbitrary positive integer.

Theorem 7.2.3. *If the integer* $n > 1$ *has a prime factorization* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, *then* $\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) = n\left(1 - \dfrac{1}{p_1}\right) \cdots \left(1 - \dfrac{1}{p_r}\right)$.

Proof. Since ϕ is multiplicative(Why!) and n has a prime factorization, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ then we have

$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_r^{\alpha_r}).$$

Again from the Theorem 7.2.1, we have $\phi(p_j^{\alpha_j}) = (p_j^{\alpha_j} - p_j^{\alpha_j - 1})$ for each

$j = 1, 2, 3, \cdots, r$. Hence

$$\begin{aligned}\phi(n) &= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

□

The exemplification of the above theorem has been done from the following example:

Example 7.2.1. *Choose* $n = 720$. *Then the prime factorization of* 720 *is* $2^4 \cdot 3^2 \cdot 5$. *Thus applying above theorem, we have*

$$\begin{aligned}\phi(360) &= 720 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right), \\ &= 720 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}, \\ &= 192.\end{aligned}$$

At the outset of this section, a table of positive integers and their corresponding phi-function, was displayed. There, $\phi(1) = \phi(2) = 1$ and the values of phi function for other integers are even. This is not a coincidence, as evident from our next theorem:

Theorem 7.2.4. *For* $n > 2$, $\phi(n)$ *is an even integer.*

Proof. Let us consider $n = 2^j$ with $j \geq 2$. Then from Theorem 7.2.1, $\phi(n) = \phi(2^j) = 2^{j-1}$, an even integer. If n is not a power of 2 then it is divisible by some odd prime. Then $n = p^j m$, where p being an odd integer and $\gcd(p, m) = 1$. Therefore $\phi(n) = \phi(p^j)\phi(m)(Why!) = p^{j-1}\phi(m)(p-1)$, which is also even(Why!). □

7.3 Worked out Exercises

Problem 7.3.1. *Verify that the equality* $\phi(z) = \phi(z+1) = \phi(z+2)$ *holds, when* $z = 5186$.

Solution 7.3.1. *Note that*

$$5186 = 2 \cdot 2593,\ \phi(5186) = 5186\left(\frac{1}{2}\right)\left(\frac{2592}{2593}\right) = 2592.$$

$$5187 = 3 \cdot 7 \cdot 13 \cdot 19,\ \phi(5187) = 5187\left(\frac{2}{3}\right)\left(\frac{6}{7}\right)\left(\frac{12}{13}\right)\left(\frac{18}{19}\right) = 2592.$$

$$5188 = 2^2 \cdot 1297,\ \phi(5188) = 5188\left(\frac{1}{2}\right)\left(\frac{1296}{1297}\right) = 2592.$$

Problem 7.3.2. *Prove: For some* $k \geq 1$, $\phi(z) = \frac{z}{2}$ *if and only if* $z = 2^k$.

Solution 7.3.2. *Let us consider* $z = 2^k$. *Then* $\phi(z) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1} = \frac{z}{2}$.

Conversely, suppose $\phi(z) = \frac{z}{2}$. *Then for* $\frac{z}{2}$ *to be an integer,* z *must be even. Let* $z = 2^k p_2^{k_2} \cdots p_r^{k_r}$ *and assume* $k_i \neq 0$. *Let* $q = p_2^{k_2} \cdots p_r^{k_r}$. *So* $q > 1$ *and* $\gcd(2^k, q) = 1$.

$$\begin{aligned}\therefore\ \phi(z) &= \phi(2^k q) = \phi(2^k)\phi(q),\\ &= 2^k\left(1 - \frac{1}{2}\right)\phi(q) = 2^{k-1}\phi(q).\\ \textit{Further } \frac{z}{2} &= \phi(z) = 2^{k-1}\phi(q) \Rightarrow z = 2^k\phi(q).\\ \therefore\ p_2^{k_2} \cdots p_r^{k_r} &= \phi(q) = \phi(p_2^{k_2} \cdots p_r^{k_r})\\ &= p_2^{k_2} \cdots p_r^{k_r}\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).\\ \therefore\ p_2 \cdots p_r &= (p_2 - 1) \cdots (p_r - 1).\end{aligned}$$

Therefore for each $p_i, p_i = (p_j - 1)$ *for some* j. *This is impossible if* $k_i \neq 0$. *Hence* $k_i = 0$. *Thus the converse part follows.*

Problem 7.3.3. *Prove that the equation* $\phi(z) = \phi(z + 2)$ *is satisfied by* $z = 2(2p - 1)$ *whenever* p *and* $2p - 1$ *are both odd primes.*

Solution 7.3.3. *Here* $2p - 1$ *is an odd prime implies* $\gcd(2, 2p - 1) = 1$.

$$\therefore\ \phi(z) = \phi(2)\phi(2p - 1) = (2p - 1)\left(1 - \frac{1}{2p - 1}\right) = 2p - 2.$$

Now $z + 2 = 2(2p - 1) + 2 = 4p$, p *being an odd prime, yields* $\gcd(4, p) = 1$.

$$\therefore\ \phi(z + 2) = \phi(4)\phi(p) = 2p\left(1 - \frac{1}{p}\right) = 2p - 2.$$

$$\therefore\ \phi(z) = \phi(z + 2).$$

Problem 7.3.4. *Show that there are infinitely many integers n for which $\phi(n)$ is a perfect square.*

Solution 7.3.4. *For $k \geq 1$, $\phi(2^k) = 2^k\left(1 - \dfrac{1}{2}\right) = 2^{k-1}$. If k is odd, then $k-1$ is even. Let $k = 2m+1$, for some $m \in \mathbb{Z}$.*

$$\therefore\ \phi(2^k) = \phi(2^{2m+1}) = (2^m)^2 = \textit{a perfect square.}$$

Thus there are infinitely many $n = 2^k$, k being odd, and $\phi(n)$ is a perfect square.

Problem 7.3.5. *Prove that if the integer n has s distinct odd prime factors, then $2^s \big| \phi(n)$.*

Solution 7.3.5. *Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $p_i > 2$.*

$$\therefore\ \phi(n) = p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1)\cdots p_s^{k_s-1}(p_s - 1).$$

As each p_i is odd, so let $p_i = 2r_i + 1$ for some r_i.

$$\begin{aligned}\therefore\ \phi(n) &= p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1)\cdots p_s^{k_s-1}(p_s - 1)(2r_1)(2r_2)\cdots(2r_s),\\ &= 2^s p_1^{k_1-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1)\cdots p_s^{k_s-1}(p_s - 1)r_1 r_2 \cdots r_s.\\ \therefore\ 2^s &\big| \phi(n).\end{aligned}$$

Problem 7.3.6. *If every prime that divides n also divides m, prove that $\phi(nm) = n\phi(m)$.*

Solution 7.3.6. *Let $p_1, p_2, \ldots, p_s$ be all those primes which divide both n and m. Suppose*

$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $m = p_1^{j_1} p_2^{j_2} \cdots p_s^{j_s} q_1^{m_1} q_2^{m_2} \cdots q_r^{m_r}$, q_i being prime be such that $q_i \neq p_j$.

$$\therefore\ nm = p_1^{k_1+j_1} p_2^{k_2+j_2} \cdots p_s^{k_s+j_s} q_1^{m_1} q_2^{m_2} \cdots q_r^{m_r}.$$

$$\begin{aligned}\therefore\ \phi(nm) &= p_1^{k_1+j_1} p_2^{k_2+j_2} \cdots p_s^{k_s+j_s} q_1^{m_1} q_2^{m_2} \cdots q_r^{m_r}\\ &\qquad \left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right)\left(1 - \frac{1}{q_1}\right)\cdots\left(1 - \frac{1}{q_r}\right),\\ &= p_1^{j_1} p_2^{j_2} \cdots p_s^{j_s}\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_s}\right)\left(1 - \frac{1}{q_1}\right)\cdots\left(1 - \frac{1}{q_r}\right) p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s},\\ &= \phi(m) p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s},\\ &= n \cdot \phi(m).\end{aligned}$$

Problem 7.3.7. *If $\phi(n) | (n-1)$, prove that n is a square-free integer.*

Solution 7.3.7. *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ *and suppose* n *is not square-free such that* $k_i \geq 2$ *for some* i. *Now*

$$\phi(n) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_i^{k_i} - p_i^{k_i - 1}) \cdots (p_s^{k_s} - p_s^{k_s - 1}).$$

Since $k_i \geq 2$, $k_i - 1 \geq 1$, *so* $p_i \big| (p_i^{k_i} - p_i^{k_i - 1}) \Rightarrow p_i \big| \phi(n)$. *By hypothesis* $\phi(n) \big| (n - 1)$ *implies* $p_i \big| (n-1)$. *Again* $p_i \big| n$ *yields* $p_i \big| n - (n-1) \Rightarrow p_i \big| 1$, *which is a contradiction. Therefore for all* i, $k_i = 1$ *implies* n *is square-free.*

Problem 7.3.8. *Prove that there are no integers* n *for which* $\phi(n) = \dfrac{n}{4}$.

Solution 7.3.8. *Here* $\phi(1) = 1 = \phi(2), \phi(3) = 2 = \phi(4)$. *So the statement holds true for* $n = 1, 2, 3, 4$. *Let* $n > 4$. *On the contrary, suppose* $\phi(n) = \dfrac{n}{4}$. *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}, k_i \geq 1$.

$$\begin{aligned}
\therefore\ \phi(n) &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) = \frac{n}{4}, \\
&\Rightarrow \frac{(p_1 - 1)(p_2 - 1) \cdots (p_s - 1)}{p_1 p_2 \cdots p_s} = \frac{1}{4}, \\
&\Rightarrow 4(p_1 - 1)(p_2 - 1) \cdots (p_s - 1) = p_1 p_2 \cdots p_s, \\
&\Rightarrow 2(p_2 - 1) \cdots (p_s - 1) = p_2 \cdots p_s,\ \textit{as } p_1 = 2.
\end{aligned}$$

Since $p_2, \ldots, p_s$ *are all odd, therefore* $p_2 \cdots p_s$ *is odd. But* $2(p_2 - 1) \cdots (p_s - 1)$ *is even. So* $p_1 = 2$ *fails to work. Now if all* $p_1, p_2, \ldots, p_s$ *are odd, then* $p_1 p_2 \cdots p_s$ *is also so. Furthermore* $4(p_1 - 1)(p_2 - 1) \cdots (p_s - 1)$ *is even, which implies no such* n *exists.*

Problem 7.3.9. *If* p *is a prime and* $k \geq 2$, *show that* $\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$.

Solution 7.3.9. *Here* $\phi(p^k) = p^{k-1}(p-1)$. *Since* $\gcd(p, p-1) = 1$, *therefore* $\gcd(p^{k-1}, p-1) = 1$. *Using the multiplicative property of* ϕ, *we obtain*

$$\phi(\phi(p^k)) = \phi(p^{k-1}(p-1)) = \phi(p^{k-1})\phi(p-1) = p^{k-2}(p-1)\phi(p-1).$$

Now for every positive integer n, $\phi(n^2) = n\phi(n)$. *Therefore* $(p-1)\phi(p-1) = \phi((p-1)^2)$. *Hence* $\phi(\phi(p^k)) = p^{k-2}(p-1)\phi(p-1) = p^{k-2}\phi((p-1)^2)$.

Problem 7.3.10. *If* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, *then prove that*

$$\sigma(n)\phi(n) \geq n^2 \left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right) \cdots \left(1 - \frac{1}{p_s^2}\right).$$

Solution 7.3.10. *Note that* $\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1}\cdots\frac{p_s^{k_s+1}-1}{p_s-1}$ *and* $\phi(n) = p_1^{k_1-1}(p_1 - 1)\cdots p_s^{k_s-1}(p_s-1)$*. Therefore* $\sigma(n)\phi(n) = (p_1^{2k_1} - p_1^{k_1-1})\cdots(p_s^{2k_s} - p_s^{k_s-1})$*. But* $(p_j^{2k_j} - p_j^{k_j-1}) = p_j^{2k_j}\left(1 - \frac{p_j^{k_j-1}}{p_j^{2k_j}}\right) = (p_j^{k_j})^2\left(1 - \frac{1}{p_j^{k_j+1}}\right)$*. For* $p_j \geq 1$ *we find*

$$p_j^{k_j+1} \geq p_j^2 \Rightarrow \frac{1}{p_j^2} \geq \frac{1}{p_j^{k_j+1}} \Rightarrow -\frac{1}{p_j^2} \leq -\frac{1}{p_j^{k_j+1}} \Rightarrow 1 - \frac{1}{p_j^2} \leq 1 - \frac{1}{p_j^{k_j+1}}.$$

$$\therefore\ p_j^{2k_j} - p_j^{k_j-1} \geq (p_j^{k_j})^2\left(1 - \frac{1}{p_j^2}\right).$$

$$\begin{aligned}\therefore\ \sigma(n)\phi(n) &\geq \prod_s (p_s^{k_s})^2\left(1 - \frac{1}{p_s^2}\right),\\ &= \prod_s (p_s^{k_s})^2 \prod_s\left(1 - \frac{1}{p_s^2}\right),\\ &= n^2\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right)\cdots\left(1 - \frac{1}{p_s^2}\right).\end{aligned}$$

7.4 Euler's Theorem

The first published proof of Fermat's little theorem(stated in chapter 5 of this book) was given by Euler in 1736, where he had taken a prime p and an integer a. But later in the year, 1760 he succeeded in generalizing the result from prime p to an arbitrary integer n. This generalization is known as Euler's generalization of Fermat's theorem. The present section deals with the proof and related ideas associated with this remarkable theorem.

Now, as a precursor to launch the proof of Euler's generalization of Fermat's theorem, we need the following lemma:

Lemma 7.4.1. *Let* $n > 1$ *and* $\gcd(a, n) = 1$*. If* $k_1, k_2, \cdots, k_{\phi(n)}$ *are the positive integers less than and prime to* n*, then* $ak_1, ak_2, \cdots, ak_{\phi(n)}$ *are congruent modulo* n *to* $k_1, k_2, \cdots, k_{\phi(n)}$ *in some order.*

Proof. Here we are going to show that no two of the integers $ak_1, ak_2, \cdots, ak_{\phi(n)}$ are congruent modulo n. For if, $ak_i \equiv ak_j \pmod{n}$ holds with $1 \leq i < j \leq \phi(n)$ then $k_i \equiv k_j \pmod{n}$, which is a contradiction since this two integers are less than n. Since, $\gcd(k_i, n) = 1\ \forall i$ and $\gcd(a, n) = 1$ then from the worked out Problem 2.6.1) $\gcd(ak_i, n) = 1\ \forall i$. Let us fix ak_j for some integer j, there exists unique integer b where $0 \leq b < n$ for which $ak_j \equiv b \pmod{n}$. Since, $\gcd(b, n) = \gcd(ak_j, n) = 1$, so b must be one of the integers $k_1, k_2, \cdots, k_{\phi(n)}$.

This is true for all j. This proves that the numbers $ak_1, ak_2, \cdots, ak_{\phi(n)}$ and the numbers $k_1, k_2, \cdots, k_{\phi(n)}$ are identical with respect to modulo n in a certain order. $\square$

We now represent an example to make a lucid understanding of this lemma. For that let us take $n = 9$ and the set $\{1, 2, 4, 5, 7, 8\}$ is a reduce system modulo 9. Since $\gcd(2, 9) = 1$ then we have, $2 \cdot 1 = 2, 2 \cdot 2 = 4, 2 \cdot 4 = 8, 2 \cdot 5 = 10, 2 \cdot 7 = 14, 2 \cdot 8 = 16$ is also a reduce system modulo 9.

Theorem 7.4.1. *(Euler): If n is a positive integer and $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (\bmod n)$.*

Now before going to the proof, we illustrate the idea of it by an example.

Example 7.4.1. *From the last example, it is clear that both the sets $\{1, 2, 4, 5, 7, 8\}$ and $\{2{\cdot}1, 2{\cdot}2, 2{\cdot}4, 2{\cdot}5, 2{\cdot}7, 2{\cdot}8\}$ are reduced residue system of modulo 9. Therefore*

$$(2 \cdot 1)(2 \cdot 2)(2 \cdot 4)(2 \cdot 5)(2 \cdot 7)(2 \cdot 8) \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 (\bmod 9),$$
$$2^6 \cdot 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \equiv 1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 (\bmod 9).$$

Since we have $\gcd(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8, 9) = 1$, we conclude that $2^6 = 2^{\phi(9)} \equiv 1 (\bmod 9)$.

We now use the idea of this example to the following proof.

Proof. Let us take $n > 1$ and $k_1, k_2, \cdots, k_{\phi(n)}$ be the positive integers less than n which are relatively prime to n. Since $\gcd(a, n) = 1$, $ak_1, ak_2, \cdots, ak_{\phi(n)}$ are congruent to $k_1, k_2, \cdots, k_{\phi(n)}$ (Why!). Then the least positive residue of $ak_1, ak_2, \cdots, ak_{\phi(n)}$ are the integers $k_1, k_2, \cdots, k_{\phi(n)}$ in some order. Therefore

$$(ak_1)(ak_2) \cdots (ak_{\phi(n)}) \equiv k_1 k_2 \cdots k_{\phi(n)} (\bmod n)$$
$$\text{and so } a^{\phi(n)} k_1 k_2 \cdots k_{\phi(n)} \equiv k_1 k_2 \cdots k_{\phi(n)} (\bmod n).$$

Since $\gcd(k_i, n) = 1$ for each i so $\gcd(k_1 k_2 \cdots k_{\phi(n)}, n) = 1$[see Problem 2.6.1]. Thus the congruence becomes $a^{\phi(n)} \equiv 1 (\bmod n)$. $\square$

Remark 7.4.1. *If $n = p$ is prime, then $\phi(p) = p - 1$. Further if $p \nmid a$, then we have $a^{p-1} \equiv 1 (\bmod p)$, which is equivalent to Fermat's Little theorem.*

Euler's theorem has vast application in finding the modulo of a large number with respect to a positive integer. Applying Euler's theorem, we can find congruent modulo of 4^{301} with respect to 99. Since $\gcd(4, 99) = 1$ and $\phi(99) = \phi(3^2 \cdot 11) = 99\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = 99 \times \frac{2}{3} \times \frac{10}{11} = 60$, from Euler's theorem we have $4^{60} \equiv 1 (\bmod 99)$. Now $301 = 5 \cdot 60 + 1$, therefore $4^{301} \equiv (4^{60})^5 \cdot 4^1 \equiv 4 (\bmod 99)$.

7.5 Worked out Exercises

Problem 7.5.1. *Use Euler's theorem to evaluate* 2^{100000} *modulo* 77.

Solution 7.5.1. *Here* $\gcd(2,77)=1$, *therefore* $2^{\phi(77)} \equiv 1 (\operatorname{mod} 77)$. *Now*

$$\phi(77) = 6 \cdot 10 = 60 \Rightarrow 2^{60} \equiv 1(\mod 77).$$

Hence

$$2^{60000} \equiv 1(\mod 77),\ (2^{60})^{300} = 2^{18000} \equiv 1(\mod 77) \Rightarrow 2^{36000} \equiv 1(\mod 77).$$
$$\therefore\ 2^{96000} \equiv 1(\mod 77),\ (2^{60})^{300} = 2^{1800} \equiv 1(\mod 77) \Rightarrow 2^{3600} \equiv 1(\mod 77).$$
$$\therefore\ 2^{99600} \equiv 1(\mod 77),\ (2^{60})^{3} = 2^{180} \equiv 1(\mod 77) \Rightarrow 2^{360} \equiv 1(\mod 77).$$
$$\therefore\ 2^{99960} \equiv 1(\mod 77).$$

But $2^{10} = 1024,\ 13 \cdot 77 = 1001 \Rightarrow 2^{10} \equiv 23 (\operatorname{mod} 77)$. *Therefore* $2^{40} \equiv 23^4 (\operatorname{mod} 77) \Rightarrow 2^{100000} \equiv 23^4 (\operatorname{mod} 77)$. *Now* $23^2 = 529 = 6 \cdot 77 + 67 \Rightarrow 23^2 \equiv -10 (\operatorname{mod} 77) \Rightarrow 23^4 \equiv 100 \equiv 23 (\operatorname{mod} 77)$. *Hence*

$$2^{100000} \equiv 23(\mod 77).$$

Problem 7.5.2. *For any prime p, prove that:*

$$\tau(p!) = 2\tau((p-1)!).$$

Solution 7.5.2. *Let* $p! = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \cdot p = 1 \cdot 2 \cdot 3 \cdots (p-1) \cdot p$ *and* $p_1, p_2, \cdots p_s$ *be distinct primes. Here* $k_i \geq 0$ *are the integers for each* $i (= 1, 2, \cdots s)$. *Therefore* $(p-1)! = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. *Since* $\gcd(p, p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) = 1$, *therefore*

$$\begin{aligned} \tau(p!) &= \tau(p \cdot p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \\ &= \tau(p)\tau(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \\ &= \tau(p)\tau((p-1)!) \\ &= 2 \cdot \tau((p-1)!),\ \because\ \tau(p) = 2. \end{aligned}$$

Problem 7.5.3. *If* $\gcd(a,n) = 1$, *show that the linear congruence* $ax \equiv b (\operatorname{mod} n)$ *has the solution* $x \equiv ba^{\phi(n)-1} (\operatorname{mod} n)$.

Solution 7.5.3. *If* $x \equiv ba^{\phi(n)-1} (\operatorname{mod} n)$, *then* $ax = a(ba^{\phi(n)-1}) = ba^{\phi(n)}$. *Since* $\gcd(a,n) = 1$, *by Euler's theorem we have* $a^{\phi(n)} \equiv 1 (\operatorname{mod} n)$.

$$\therefore\ ax = ba^{\phi(n)} \equiv b \cdot 1 \equiv b(\mod n).$$

Problem 7.5.4. *Show that if* $\gcd(a,n) = gcd(a-1,n) = 1$, *then*

$$1 + a + a^2 + \ldots + a^{\phi(n)-1} \equiv 0(\mod n).$$

Solution 7.5.4. *By Euler's theorem, we have*

$$\gcd(a,n)=1 \Rightarrow a^{\phi(n)} \equiv 1(\bmod n) \Rightarrow a^{\phi(n)}-1 \equiv 0(\bmod n).$$

But $a^{\phi(n)}-1=(a-1)(a^{\phi(n)-1}+\ldots+a^2+a+1)$*. Therefore* $(a-1)(a^{\phi(n)-1}+\ldots+a^2+a+1) \equiv 0(\bmod n)$*. Since* $\gcd(a-1,n)=1$*, therefore* $1+a+a^2+\ldots+a^{\phi(n)-1} \equiv 0(\bmod n)$*.*

Problem 7.5.5. *If* m *and* n *are relatively prime positive integers, prove that* $m^{\phi(n)}+n^{\phi(m)} \equiv 1(\bmod mn)$*.*

Solution 7.5.5. *Since* $\gcd(m,n)=1$*, therefore an appeal to Euler's theorem produces*

$$m^{\phi(n)} \equiv 1(\bmod n) \;\&\; n^{\phi(m)} \equiv 1(\bmod m).$$

But $n^{\phi(m)} \equiv 0(\bmod n)$ & $m^{\phi(n)} \equiv 0(\bmod m)$*.*

$$\begin{aligned}\therefore\; m^{\phi(n)}+n^{\phi(m)} &\equiv 1+0=1(\bmod n),\\ n^{\phi(m)}+m^{\phi(n)} &\equiv 1+0=1(\bmod m).\end{aligned}$$

Since $\gcd(m,n)=1$*, therefore combining we obtain* $m^{\phi(n)}+n^{\phi(m)} \equiv 1(\bmod mn)$*.*

Problem 7.5.6. *Find the units digit of* 3^{100} *by means of Euler's theorem.*

Solution 7.5.6. *Here* $\gcd(10,3)=1$*. By Euler's theorem,* $3^{\phi(10)} \equiv 1(\bmod 10)$*. Now,* $\phi(10)=4$*, therefore* $3^4 \equiv 1(\bmod 10)$*. Hence* $(3^4)^{25} \equiv 1(\bmod 10)$*. Therefore* $3^{100} \equiv 1(\bmod 10)$*. Thus, unit digit of* 3^{100} *is* 1*.*

Problem 7.5.7. *Prove that* $a^{15} \equiv a^3(\bmod (2^{15}-2^3))$ *for any integer* a*.*

Solution 7.5.7. *Here,*

$$\begin{aligned}a^{15}-a^3 &= a^3(a^{12}-1)=a^3(a^6+1)(a^6-1)\\ &= a^3(a^6+1)((a^3+1))(a^3-1)\\ &= a^3(a^6+1)((a^3+1))(a^2+a+1)(a-1).\\ 2^{15}-2^3 &= 2^3(2^6+1)((2^3+1))(2^2+2+1)(2-1)\\ &= 2^3\cdot 3^2\cdot 5\cdot 7\cdot 13.\end{aligned}$$

Applying the definition of Euler's phi function we get,

$$\phi(8)=4, \phi(5)=4, \phi(13)=12, \phi(9)=6, \phi(7)=6.$$

Case(i) *If* $\gcd(a,2^{15}-2^3)=1$*, then this implies,*

$$\gcd(a,8)=1, \qquad \gcd(a,13)=1, \qquad \gcd(a,2)=1,$$

$$\gcd(a,5)=1, \qquad \gcd(a,9)=1.$$

Now applying Euler's theorem in all those above cases we can write,

$$a^4 \equiv 1(\bmod 8), \qquad a^{12} \equiv 1(\bmod 13), \qquad a^6 \equiv 1(\bmod 7),$$

$$a^4 \equiv 1(\bmod 5), \qquad a^6 \equiv 1(\bmod 9).$$

Considering all the congruences together, we have

$$a^{12} \equiv 1(\bmod 8\cdot 5\cdot 13\cdot 9\cdot 7).$$

$$\therefore\ a^{15} \equiv a^3(\bmod (2^{15}-2^3)).$$

Case(ii) *If* $\gcd(a, 2^{15}-2^3) \neq 1$, *then for some integer* k,

$$a = k(2^{15}-2^3),\ \textit{and}$$

$$a^{15}-a^3 = (a^{14}-a^2)a = (a^{14}-a^2)k(2^{15}-2^3) \Rightarrow a^{15} \equiv a^3(\bmod (2^{15}-2^3)).$$

Hence combining both the cases for any integer a*, we get* $a^{15} \equiv a^3(\text{mod } (2^{15}-2^3))$.

Problem 7.5.8. *Use Euler's theorem to confirm that, for any integer* $z \geq 0,\ 51|10^{32z+9}-7$.

Solution 7.5.8. *Here,* $51 = 17\cdot 3$. *Therefore* $\phi(51) = 16\cdot 2 = 32$. *Also,* $\gcd(10,51)=1$ *gives* $10^{\phi(51)} = 10^{32} \equiv 1(\text{mod } 51)$. *Thus,*

$$10^{32z} \equiv 1(\bmod 51). \tag{7.5.1}$$

Next, we are going to show $10^9 \equiv 7(\text{mod } 51)$. *Now,*

$$10 \equiv 7(\bmod 3),$$

$$10 \equiv 1(\bmod 3) \Rightarrow 10^{18} \equiv 1(\bmod 3).$$

$$\therefore\ 10^9 = 10^8\cdot 10 \equiv 7\cdot 1(\bmod 3),$$

$$\textit{or, } 10^9 \equiv 7(\bmod 3). \tag{7.5.2}$$

$$-10 \equiv 7(\bmod 17),$$

$$\therefore\ (-10)^2 \equiv 7^2 = 49 \equiv -2(\bmod 17).$$

$$\therefore\ (-10)^8 = 10^8 \equiv (-2)^4 = 16 \equiv -1(\bmod 17).$$

$$\therefore\ (-10)^9 \equiv -10 \equiv 7(\bmod 17). \tag{7.5.3}$$

$$(7.5.2)+(7.5.3) \Rightarrow 10^9 \equiv 7(\bmod 51). \tag{7.5.4}$$

$$(7.5.1)+(7.5.4) \Rightarrow 10^{32z}\cdot 10^9 \equiv 1\cdot 7(\bmod 51),$$

$$10^{32z+9} \equiv 7(\bmod 51). \tag{7.5.5}$$

Thus, for any integer $z \geq 0,\ 51|10^{32z+9}-7$.

Problem 7.5.9. *Prove that if* a *is an integer, then* $a^7 \equiv a(\bmod 63)$.

Solution 7.5.9. *From Fermat's little theorem we see that,* $a^7 \equiv a(\bmod 7)$. *So to prove this assertion we need to check* $a^7 \equiv a(\bmod 9)$. *If* $9|a$ *then it is trivial. If* $3 \nmid a$ *then* $\gcd(a, 9) = 1$, *so from Euler's theorem it follows that* $a^{\phi(9)} = a^6 \equiv 1(\bmod 9)$ *or* $a^7 \equiv a(\bmod 9)$. *Thus together we have* $a^7 \equiv a(\bmod 63)$.

Problem 7.5.10. *Solve the linear congruence* $5x \equiv 3(\bmod 14)$ *by Euler's theorem.*

Solution 7.5.10. *Here we multiply both sides of the congruence by* $5^{\phi(14)-1} = 5^5$. *This gives* $5^6 \cdot x \equiv 3 \cdot 5^5(\bmod 14)$. *Now by Euler's theorem we have* $5^{\phi(14)} = 5^6 \equiv 1(\bmod 14)$. *This implies,* $x \equiv 3 \cdot 5^5 \equiv 15 \cdot 11^{11} \equiv 15 \cdot 9 \equiv 9(\bmod 14)$.

7.6 Properties of ϕ–function

Present section deals with some curious properties of Euler's phi function related with some arithmetic functions. Discussion of this chapter commence with an important property of totient(ϕ) function, where the sum of values of $\phi(d)$ where d is the divisor of any positive integer n is always equal to n itself. Famous German mathematician Carl Friedrich Gauss was the first person to notice that.

Theorem 7.6.1. *For each positive integer* $n \geq 1, n = \sum_{d|n} \phi(d)$ *where* d *is positive divisor of* n.

Proof. Let us choose $n = 1$ then, $\sum_{d|1} \phi(d) = \phi(1) = 1 = n$. Thus the equality is true in this case. Now we are only to prove the result for any positive integer $n > 1$. Let us choose a set $S_n = \{1, 2, 3, \cdots, n\}$ and $|S_n|$ be the number of elements in S_n, then clearly $|S_n| = n$. For each divisor d of n we denote S_d be the set of all integers not exceeding n and $\gcd(m, n) = d$ for each $m \in S_d$. Now from the proposition (2.4.2) we have $\gcd(m, n) = d$ if and only if $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. We now have to show that each S_d has $\phi\left(\frac{n}{d}\right)$ number of elements. Here for a particular d all the elements of S_d are multiples of d and less than or equal to n. Thus the elements of S_d are $d, 2d, 3d, \cdots, \left(\frac{n}{d}\right)d$. Now, let $ad \in S_d$ be any element where $\gcd\left(a, \frac{n}{d}\right) = e$. Then clearly $\gcd(ad, n) = ed$. Here $ed = d$ if and only if $e = 1$ imply that only ad in S_d are those whose $\gcd\left(a, \frac{n}{d}\right) = 1$ that is the number $\phi\left(\frac{n}{d}\right)$. Since each integers of the set $\{1, 2, 3, \cdots, n\}$ lies in exactly one class S_d, we have the formula $n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$. But d runs through all positive divisors of n so does $\frac{n}{d}$. Thus finally we have, $n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$. □

Here we have illustrated the above theorem by means of an example:

Example 7.6.1. *Let us choose a number* $n = 12$ *and the divisors of* 12 *are* $1, 2, 3, 4, 6, 12$. *Thus the classes* S_d *are,*

$$S_1 = \{1, 5, 7, 11\}, S_2 = \{2, 10\}, S_3 = \{3, 9\}, S_4 = \{4, 8\}, S_6 = \{6\} S_{12} = \{12\}.$$

Now, $\phi(12) = 4, \phi(6) = 2, \phi(4) = 2, \phi(3) = 2, \phi(2) = 1, \phi(1) = 1$.

Therefore $\sum_{d|12} \phi(12) = \phi(12) + \phi(6) + \phi(4) + \phi(3) + \phi(2) + \phi(1) = 12 = n$.
This shows the clarification of our above theorem.

Also, the next part of our discussion is based on the last theorem. Here we illustrate the theorem with a suitable example, which totally depends on the multiplicative property of ϕ[for further details refer to theorem (7.2.2)]. Now for $n = 1$, the case is trivial. Let us choose $n = 24$ and apply the formula $F(n) = \sum_{d|n} \phi(d)$ where F and ϕ are both number theoretic functions. Since ϕ is multiplicative, F is also so(Why!). Again $n = 24 = 2^3 \cdot 3$ be the prime factorization of 24, which implies $F(24) = F(2^3)F(3)$. Now

$$\begin{aligned}
F(2^3) &= \sum_{d|2^3} \phi(d) \\
&= \phi(1) + \phi(2) + \phi(4) + \phi(8) \\
&= 1 + (2-1) + (2^2 - 2) + (2^3 - 2^2)[\because \phi(p^k) = p^k - p^{k-1}] \\
&= 1 + 1 + 2 + 4 = 2^3 \\
\text{and } F(3) &= \sum_{d|3} \phi(d) \\
&= \phi(1) + \phi(3) = 1 + 2 = 3.
\end{aligned}$$

Therefore $F(24) = 2^3 \cdot 3 = 24$ and thus we have $n = 24 = F(24) = \sum_{d|24} \phi(d)$ which is our desired result.

Based on the last example, we are going to give the alternative proof of Theorem 7.6.1 as follows:

Proof. If $n = 1$, the case is trivial(Verify!). So we assume $n > 1$. Let us consider the number-theoretic function $F(n) = \sum_{d|n} \phi(d)$. Since ϕ is multiplicative, F is also so. Let the prime factorization of n be given by $n = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$. Then $F(n) = F(p_1^{d_1})F(p_2^{d_2}) \cdots F(p_s^{d_s})$. For each value of j, we obtain

$$\begin{aligned} F(p_j^{d_j}) &= \sum_{d|p_j^{d_j}} \phi(d) \\ &= \phi(1) + \phi(p_j) + \phi(p_j^2) + \phi(p_j^3) + \ldots + \phi(p_j^{d_j}) \\ &= 1 + (p_j - 1) + (p_j^2 - p_j) + (p_j^3 - p_j^2) + \ldots + (p_j^{d_j} - p_j^{d_j - 1}) \\ &= p_j^{d_j}. \end{aligned}$$

Hence $F(n) = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s} = n \Rightarrow \sum_{d|n} \phi(d) = n.$ □

Now for the next part of discussion , let us choose a positive integer 20 and $\phi(20) = 8$. Here the set of positive integers less than 20 and prime to 20 are $\{1, 3, 7, 9, 11, 13, 17, 19\}$ and their sum is $1+3+7+9+11+13+17+19 = 80 = \frac{1}{2} \times 20 \times 8$. This is not a coincidence, in fact our next theorem deals with it.

Theorem 7.6.2. *For $n > 1$, the sum of the positive integers less than n and prime to n is $\frac{1}{2}n\phi(n)$.*

Proof. Let $k_1, k_2, \cdots, k_{\phi(n)}$ be the positive integers less than n and prime to n. Now using Proposition (2.4.3), we have from congruence relation,

$$\begin{aligned} k_1 + k_2 + \cdots + k_{\phi(n)} &= (n - k_1) + (n - k_2) + \cdots + (n - k_{\phi(n)}) \\ &= n\phi(n) - (k_1 + k_2 + \cdots + k_{\phi(n)}) \end{aligned}$$

$$\text{Therefore,}\quad 2(k_1 + k_2 + \cdots + a_{\phi(n)}) = n\phi(n)$$
$$\Rightarrow k_1 + k_2 + \cdots + k_{\phi(n)} = \frac{1}{2}n\phi(n),$$

which proves the theorem. □

Finally at this point we can give an application of Mobiöus Inversion formula, which leads us to the following theorem:

Theorem 7.6.3. *For any positive integer n, $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.*

Before going to the proof, let us illustrate the theorem by means of an example: taking $n = 14$ we see that,

$$\begin{aligned}14\sum_{d|14}\left(\frac{\mu(d)}{d}\right) &= 14\left[\mu(1)+\frac{\mu(2)}{2}+\frac{\mu(7)}{7}+\frac{\mu(14)}{14}\right]\\ &= 14\left[1+\frac{-1}{2}+\frac{(-1)}{7}+\frac{(-1)^2}{14}\right]\\ &= 14\left[1-\frac{1}{2}-\frac{1}{7}+\frac{1}{14}\right]\\ &= 14\times\frac{6}{14}=6=\phi(14).\end{aligned}$$

Proof. From the Theorem (7.6.1) we know, $F(n)=\sum_{d|n}\phi(d)=n$ and from Mobiöus inversion formulae we have, $\phi(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)$. Therefore we get, $\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}=n\sum_{d|n}\frac{\mu(d)}{d}$. □

7.7 Worked out Exercises

Problem 7.7.1. *For a square-free integer $n>1$, show that $\tau(n^2)=n$ if and only if $n=3$.*

Solution 7.7.1. *If $n=3$, then $\tau(n^2)=\tau(3^2)=2+1=3$[refer to Theorem 6.2.2]. Next, suppose n is square-free with $n>1$ and $\tau(n^2)=n$. Let $n=p_1p_2\cdots p_s$ with $p_i\neq p_j$. Moreover, applying Theorem 6.2.2 we get*

$$\begin{aligned}\tau(n^2)&=\tau(p_1^2p_2^2\cdots p_s^2)\\ &=(2+1)(2+1)\cdots(2+1)=3^s.\\ \therefore\ \tau(n^2)&=n=p_1p_2\cdots p_s=3^s,\end{aligned}$$

which implies all $p_i=3$. Hence $n=3$ and $s=1$.

Problem 7.7.2. *For $n>2$, prove the inequality $\phi(n^2)+\phi((n+1)^2)\leq 2n^2$.*

Solution 7.7.2. *If k is composite, then $\phi(k)\leq k-\sqrt{k}$. As n^2 is composite, so is $(n+1)^2$. Therefore $\phi(n^2)\leq n^2-\sqrt{n^2}=n^2-n$. Again $\phi((n+1)^2)\leq(n+1)^2-\sqrt{(n+1)^2}=n^2+n$. Thus $\phi(n^2)+\phi((n+1)^2)\leq 2n^2$.*

Problem 7.7.3. *Given an integer z, prove that there exists at least one k for which $z|\phi(k)$.*

Solution 7.7.3. *Let* $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *be such that*

$$\phi(k) = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}(p_1 - 1) \cdots (p_r - 1).$$

Our claim is $z = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r - 1}$*. So let* $z = q_1^{\beta_1} \cdots q_s^{\beta_s}$*. Choose* $k = q_1^{\beta_1 + 1} \cdots q_s^{\beta_s + 1}$*.*

$$\therefore\ \phi(k) = q_1^{\beta_1} \cdots q_s^{\beta_s}(q_1 - 1) \cdots (q_s - 1),$$

which implies $z | \phi(k)$*.*

Problem 7.7.4. *Show that if* z *is a product of twin primes, say* $z = p(p+2)$*, then*

$$\phi(z)\sigma(z) = (z+1)(z+3).$$

Solution 7.7.4. *Here* $\gcd(p, p+2) = 1$*, so* $\phi(z) = \phi(p)\phi(p+2) = (p-1)(p+1)$*. But* $\sigma(z) = \sigma(p)\sigma(p+2) = (p+1)(p+3)$*. Therefore* $\phi(z)\sigma(z) = (p-1)(p+1)^2(p+3)$*. Now* $(z+1)(z-3) = (p^2+2p+1)(p^2+2p-3) = (p+1)^2(p+3)(p-1)$*. Hence* $\phi(z)\sigma(z) = (z+1)(z+3)$*.*

Problem 7.7.5. *Assuming* $d|n$*, prove that* $\phi(d)|\phi(n)$*.*

Solution 7.7.5. *Since* $d|n$*, so assume* $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *and* $d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ *where* $0 \leq a_i \leq k_i$*. Then* $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$ *and* $\phi(d) = d(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r})$*. Since* $d|n$*, then it follows that* $\phi(d)|\phi(n)$*.*

Problem 7.7.6. *If* z *is a square-free integer, prove that for all integers* $k \geq 2$

$$\sum_{d|z} \sigma(d^{k-1})\phi(d) = z^k.$$

Solution 7.7.6. *Since* ϕ *and* σ *are multiplicative,*

$$F(z) = \sum_{d|z} \sigma(d^{k-1})\phi(d) = \sum_{d|z} \underbrace{\sigma(d)\sigma(d) \cdots \sigma(d)}_{(k-1)\,times} \phi(d),$$

is also so.

Case(i) *Let* z *be square-free and* $z = p$*. Then*

$$\begin{aligned} F(p) &= \sum_{d|z} \sigma(d^{k-1})\phi(d) \\ &= \sigma(1)\phi(1) + \sigma(p^{k-1})\phi(p) \\ &= 1 + \frac{p^{k-1+1} - 1}{p - 1} \cdot (p-1) = p^k = z^k. \end{aligned}$$

Case(ii) *If* $z = p_1 p_2 \cdots p_r$, *then*

$$\begin{aligned}\sum_{d|z} \sigma(d^{k-1})\phi(d) &= F(z) = F(p_1)F(p_2)\cdots F(p_r)\\ &= p_1^k p_2^k \cdots p_r^k = (p_1 p_2 \cdots p_r)^k = z^k.\end{aligned}$$

Problem 7.7.7. *For any integer* n, *prove that* $3|\sigma(3n+2)$.

Solution 7.7.7. *Let* $3n+2 = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. *Since* $3 \equiv 0(\bmod 3)$ *and* $3n+2 \equiv 2(\bmod 3)$, *therefore* $p_i^{k_i} \not\equiv 0(\bmod 3)$ *for* $i = 1, 2, \ldots, s$. *If all* $p_i^{k_i} \equiv 1(\bmod 3)$, *then* $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \equiv 1(\bmod 3)$. *Since* $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \equiv 2(\bmod 3)$, *therefore* $\exists$ *one* p_i *satisfying* $p_i^{k_i} \equiv 2(\bmod 3)$. *This implies* $p_i \equiv 2(\bmod 3)$. *Because if* $p_i \equiv 0(\bmod 3)$ *and* $p_i \equiv 1(\bmod 3)$, *then this yields* $p_i^{k_i} \equiv 0(\bmod 3)$ *and* $p_i^{k_i} \equiv 1(\bmod 3)$ *respectively. But this is not the case. Since* $p_i \equiv 2(\bmod 3)$, *then* $p_i^2 \equiv 4 \equiv 1(\bmod 3)$ *and* $p_i^3 \equiv 2(\bmod 3)$. *Therefore if* $p_i^r \equiv 2(\bmod 3)$, *then* r *is odd. Hence* $p_i^{k_i} \equiv 2(\bmod 3)$, k_i *is odd.*

$$\begin{aligned}\therefore\ \sigma(p_i^{k_i}) = \frac{p_i^{k_{i+1}} - 1}{p_i - 1} &= \frac{(p_i - 1)(p_i^{k_i} + p_i^{k_i - 1} + \ldots + p_i + 1)}{p_i - 1},\\ &= p_i^{k_i} + p_i^{k_i - 1} + \ldots + p_i + 1, \text{ and } k_i \text{ is odd.}\end{aligned}$$

Since $2 \equiv (-1)(\bmod 3)$, *therefore if* r *is odd then* $p_i^r \equiv (-1)(\bmod 3)$ *and if* r *is even then* $p_i^r \equiv 1(\bmod 3)$.

$$\begin{aligned}\therefore\ \sigma(p_i^{k_i}) &= p_i^{k_i} + p_i^{k_i - 1} + \ldots + p_i + 1\\ &\equiv (-1) + 1 + \ldots + (-1) + 1(\bmod 3)\\ &\equiv 0(\bmod 3.).\\ \therefore\ 3|\sigma(p_i^{k_i}) &\Rightarrow 3|(\sigma(p_1^{k_1}))\cdots\sigma(p_i^{k_i})\cdots\sigma(p_s^{k_s})\\ &\Rightarrow \sigma(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}),\ \because,\ \sigma \text{ is multiplicative}\\ &3|\sigma(3n+2).\end{aligned}$$

Problem 7.7.8. *For any integer* $n > 1$ *has the form* $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, *then show that* $\sum_{d|n} \mu(d)\phi(d) = (2 - p_1)(2 - p_2)\ldots(2 - p_r)$.

Solution 7.7.8. *Since* μ *and* ϕ *are multiplicative then* $\mu \cdot \phi$ *is also multiplicative. Therefore* $F(n) = \sum_{d|n} \mu(d)\phi(d)$ *is also multiplicative. Note that* $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ *is the prime factorization of* n. *Then*

$$\begin{aligned}F(p^k) &= \sum_{d|p^k} \mu(d)\phi(d)\\ &= \mu(1)\phi(1) + \mu(p)\phi(p) + \ldots + \mu(p^k)\phi(p^k)\\ &= 1 + (-1)(p-1) = 2 - p\ [\because \mu(p^k) = 0 \text{ for } k \geq 2].\end{aligned}$$

$\therefore\ F(n) = (2-p_1)(2-p_2)\ldots(2-p_r).$

Problem 7.7.9. *If the integer* $z > 1$ *has the prime factorization* $z = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$, *prove*

$$\sum_{d|z} d\phi(d) = \left(\frac{q_1^{2k_1+1}+1}{q_1+1}\right)\left(\frac{q_2^{2k_2+1}+1}{q_2+1}\right)\cdots\left(\frac{q_s^{2k_s+1}+1}{q_s+1}\right).$$

Solution 7.7.9. *Since* $f(x) = x$ *is multiplicative, therefore* $f \cdot \phi$ *is also so. Hence*

$$F(z) = \sum_{d|z} d\phi(d), \text{ is multiplicative.}$$

Consider,

$$\begin{aligned}
F(q^k) &= \sum_{d|q^k} d\phi(d)\\
&= 1\cdot\phi(1) + q\cdot\phi(q) + q^2\cdot\phi(q^2) + \ldots + q^k\cdot\phi(q^k),\\
&= 1 + q(q-q^0) + q^2(q^2-q) + \ldots + q^k(q^k - q^{k-1}),\\
&= 1 + q^2 - q + q^4 - q^3 + q^6 - q^5 + \ldots + q^{2k} - q^{2k-1},\\
&= 1 + (-1)^1 q + (-1)^2 q^2 + (-1)^3 q^3 + \ldots + (-1)^{2k} q^{2k}.
\end{aligned}$$

$$\therefore\ q^{2k+1} + 1 = (q+1)(q^{2k} - q^{2k-1} + \ldots + q^2 - q + 1)(Why!).$$

$$\Rightarrow\ \frac{q^{2k+1}+1}{q+1} = q^{2k} - q^{2k-1} + \ldots + q^2 - q + 1,$$

$$\Rightarrow\ F(q^k) = \frac{q^{2k+1}+1}{q+1}.$$

$$\begin{aligned}
\therefore\ \sum_{d|z} d\phi(d) &= F(z) = F(q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}),\\
&= F(q_1^{k_1})F(q_2^{k_2})\cdots F(q_s^{k_s}),\\
&= \left(\frac{q_1^{2k_1+1}+1}{q_1+1}\right)\left(\frac{q_2^{2k_2+1}+1}{q_2+1}\right)\cdots\left(\frac{q_s^{2k_s+1}+1}{q_s+1}\right).
\end{aligned}$$

Problem 7.7.10. *Given* $k > 0$, *establish that there exists a sequence of* k *consecutive integers* $n+1, n+2, \ldots, n+k$ *satisfying*

$$\mu(n+1) = \mu(n+2) = \cdots = \mu(n+k) = 0.$$

Solution 7.7.10. *Let* p_k *be the* k*th prime. Then for* $i \neq j$. $\gcd(p_i^2, p_j^2) = 1$. *By* *virtue of Chinese Remainder theorem,* $\exists$ *a solution to:*

$$\begin{aligned} X &\equiv -1(\mod p_1^2),\\ X &\equiv -2(\mod p_2^2),\\ &\vdots\\ X &\equiv -k(\mod p_k^2), \end{aligned}$$

where $p_1 = 2, p_2 = 3, \ldots, p_k = k$*th prime. If* $n = p_1 p_2 \cdots p_k$ *and* $N_i = \frac{n}{p_i}$*, then a simultaneous solution is*

$$\begin{aligned} X &= (-1)N_1^{\phi(p_1^2)} + (-2)N_2^{\phi(p_2^2)} + \ldots + N_k^{\phi(p_k^2)}.\\ \Rightarrow X &= -N_1^{\phi(2^2)} - 2N_2^{\phi(3^2)} - \ldots - kN_k^{\phi(k^2)}.\\ \Rightarrow X + i &\equiv 0(\mod p_i^2),\ \textit{for}\ \ i = 1, 2, 3, \ldots, k.\\ \Rightarrow X + i &= ap_i^2,\ \textit{for some integer}\ \ a. \end{aligned}$$

Hence $\mu(X + i) = 0,\ i = 1, 2, 3, \ldots, k.$

7.8 Exercises:

1. Calculate $\phi(5040)$, $\phi(36000)$.

2. Prove the following assertions:
   (a) $\phi(3n) = 3\phi(n)$ if and only if $3|n$.
   (b) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.

3. If the integer $n > 1$ has r distinct prime factors, then show that $\phi(n) \geq \frac{n}{2^r}$.

4. If $n = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}$ then prove the inequality $\tau(n)\phi(n) \geq n$.

5. Prove that there are infinitely many integers n satisfying $\phi(n) = \frac{n}{3}$.

6. Show that Goldbach's Conjecture implies that for each even integer $2n$ there exists integers n_1 and n_2 with $\phi(n_1) + \phi(n_2) = 2n$.

7. Use Euler's theorem to establish the following:
   (a) For any integer a, $a^{13} \equiv a(\mod 2730)$.
   (b) For any odd integer a, $a^{33} \equiv a(\mod 4080)$.

8. For any prime p prove the following assertions:
   (a) $\sigma(p!) = (p + 1)\sigma((p - 1)!)$;
   (b) $\phi(p!) = (p + 1)\phi((p - 1)!)$.

9. Prove that $4|\sigma(4n+3)$ for any positive integer n.

10. If the integer $n > 1$ has the prime factorization $n = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$ then establish that:
$\sum_{d|n} \frac{\phi(d)}{d} = (1 + \frac{k_1(p_1-1)}{p_1})(1 + \frac{k_2(p_2-1)}{p_2}) \dots (1 + \frac{k_r(p_r-1)}{p_r})$.

11. Show that for any integer n, $\phi(n)|n-1$ if and only if n is prime.

12. Prove that $\sum_{d|n} \sigma(d)\phi(\frac{n}{d}) = n\tau(n)$.

13. For a positive integer z, prove that $\displaystyle\sum_{d|z} \frac{\mu^2(d)}{\phi(d)} = \frac{z}{\phi(z)}$.

14. Show that if p and $2p+1$ are both odd primes, then $n = 4p$ satisfies $\phi(n+2) = \phi(n) + 2$.

15. For which positive integer n does $\phi(n)$ divides n?

8

Primitive Roots

> *"The mathematician Pascal admires the beauty of a theorem in number theory; it's as though he were admiring a beautiful natural phenomenon. Its marvellous, he says, what wonderful properties numbers have. It's as though he were admiring the regularities in a kind of crystal."*
>
> – Ludwig Wittgenstein

8.1 Introduction

In this chapter we have studied another important aspect of modular arithmetic called primitive root. To study primitive roots we have introduced the concept of order of an integer modulo $k(\in \mathbb{Z}^+)$. The order of an integer a modulo k is the least positive integer t for which $a^t \equiv 1(\bmod\ k)$, where $\gcd(a, k) = 1$. Basically for this value of k, a becomes the primitive root of k if t becomes $\phi(k)$. For instance 3 is a primitive root of 5, because $3^{\phi(5)} = 3^4 = 81 \equiv 1(\bmod\ 5)$.

When primitive root exists, it is very convenient to apply them in proofs and explicit constructions; for instance if p is an odd prime and a is a primitive root modulo p, the quadratic residues modulo p are exactly the even powers of the primitive root.

Another important usefulness of primitive roots is to find indices or discrete logarithms of integers. This discrete logarithm which follows similar properties as logarithm of positive real numbers, can be applied in simplifying the computations of modular arithmetic.

The primitive root modulo k is mainly used in Cryptography, including the Diffi-Hellman key exchange. Also primitive roots are applicable in sound diffusers.

8.2 Multiplicative Order

In the last chapter we have seen that for any integer a and positive integer m with $\gcd(a,m) = 1$, $a^{\phi(m)} \equiv 1(\text{mod } m)$ where $\phi(m)$ is Euler's phi function. Thus there exists at least one integer x which satisfies the equation $a^x \equiv 1(\text{mod } m)$. Then from well ordering principle we can assert that there exists a least positive integer n which satisfies the above congruence equation. This leads to the following definition.

Definition 8.2.1. *Let $m > 1$ and there exists an integer a such that $\gcd(a,m) = 1$. Then the least positive integer x which satisfies the equation $a^x \equiv 1(\text{mod } m)$ is called order of integer a modulo m, denoted by $ord_m a$. In 1801 Gauss introduced this notation in his text book Disquisitiones Arithmeticae.*

Example 8.2.1. *Here, our goal is to find an order of 3 modulo 11. We have $3^5 = 243 \equiv 1(\text{mod } 11)$. Therefore the integer 3 has order 5 modulo 11.*

In above example, if we consider $3^{10}, 3^{15}$ or powers in terms of multiple of 5 then those values will also satisfy the equation $3^x \equiv 1(\text{mod } 11)$. Our next theorem deals with this fact.

Theorem 8.2.1. *If $a(\in \mathbb{Z})$ has order n modulo m i.e. $ord_m a = n$ then, $a^b \equiv 1(\text{mod } m)$ holds if and only if n divides b.*

Proof. Suppose n divides b. So b can be written as $b = kn$ for some integer k. Since $ord_m a = n$ then,

$$a^n \equiv 1(\text{ mod } m) \Rightarrow (a^n)^k \equiv 1^k(\text{ mod } m) \text{ or } a^b \equiv 1(\text{ mod } m).$$

Conversely, let b be a positive integer satisfying $a^x \equiv 1(\text{mod } m)$. Then by the division algorithm $\exists\ q, r$ such that $b = qn + r,\ 0 \leq r < n$. Therefore $a^b = (a^n)^q.a^r$. Now $a^b \equiv 1(\text{mod } m)$ and $a^n \equiv 1(\text{mod } m)$ together implies $a^r \equiv 1(\text{mod } m)$, which contradicts the fact that n is the least positive integer. Therefore we have $b = qn$ and consequently $n|b$. This proves the theorem. □

An immediate consequence of the last theorem leads to the following corollary.

Corollary 8.2.1. *If a and m are relatively prime with $m > 0$ then, order of the integer a modulo m must divides $\phi(m)$ i.e. $ord_m a \big| \phi(m)$.*

Proof. We know that $\gcd(a, m) = 1$. Then by Euler's theorem, $a^{\phi(m)} \equiv 1(\bmod m)$ satisfies the equation $a^x \equiv 1(\bmod m)$. If k be the order of a modulo m *i.e.* $ord_m a = k$ then, k must divide $\phi(m)$. □

We now illustrate the fact by means of an example. For that, let us choose $a = 5$ and $m = 12$. Then the integers less than 12 and prime to 12 are $1, 5, 7, 11$. Thus, $\phi(12) = 4$. It is easy to see that $5^2 \equiv 1(\bmod 12) \Rightarrow ord_{12} 5 = 2$. Obviously 2 divides $4 = \phi(12)$. Then we can write this as $5^4 \equiv 5^2(\bmod 12)$ where $4 \equiv 2(\bmod 2)$. Our next result is based on the order of an integer.

Theorem 8.2.2. *If a has order n modulo m i.e. $ord_m a = n$ then, for some non negative integers i and j the congruence $a^i \equiv a^j(\bmod m)$ holds if and only if $i \equiv j(\bmod n)$ prevails.*

Proof. To start with, assume $a^i \equiv a^j(\bmod m)$ where $i \geq j$. Since $\gcd(a, m) = 1$ then, $a^{i-j} \equiv 1(\bmod m)$(Why?). As a has order n modulo m so, $n \big| (i - j)$[refer to Theorem 8.2.1]. Therefore $i \equiv j(\bmod n)$.

For the converse part, let $i \equiv j(\bmod n)$. Then $i = qn + j$ for some integer q. Also, $a^n \equiv 1(\bmod m)$. This shows that $a^i = a^{nq+j} = (a^n)^q \cdot a^j \equiv a^j(\bmod m)$. This finishes the proof. □

Theorem 8.2.2 gives an idea about the exponent x of a which satisfies $a^x \equiv 1(\bmod m)$. Now a fairly natural question presents itself: Is it possible to express the order of any exponent of a in terms of order a? The following theorem contains the answer.

Theorem 8.2.3. *If the integer a has order n modulo m, then a^t has order $\dfrac{n}{\gcd(t, n)}$ modulo m for some $t > 0$. In other words, for some $t > 0$ if $ord_m a = n$ then $ord_m a^t = \dfrac{n}{\gcd(t, n)}$.*

Proof. Let $d = \gcd(t, n)$. Then $t = b_1 d$, $n = b_2 d$ with $\gcd(b_1, b_2) = 1$ for some integers b_1 and b_2. Now $(a^t)^{b_2} = (a^{b_1 d})^{\frac{n}{d}} = (a^n)^{b_1} \equiv 1(\bmod m)$. If a^t is assumed to have order r modulo m then by Theorem 8.2.1, we have $r|b_2$. On the other hand, since a has order n modulo m, the congruence $a^{tr} = (a^t)^r \equiv 1(\bmod m)$ indicates $n|tr$. This yields $b_2 d \big| b_1 dr \Rightarrow b_2 \big| b_1 r$. Now $\gcd(b_1, b_2) = 1$ shows $b_2|r$. Also, $r\big|b_2$ and $b_2\big|r$ simultaneously implies $r = b_2 = \dfrac{n}{d} = \dfrac{n}{\gcd(t, n)}$. Therefore a^t has order $\dfrac{n}{\gcd(t, n)}$ modulo m. □

We take immediate advantage of this theorem to prove the following corollary.

Corollary 8.2.2. *Let* $a(\in \mathbb{Z})$ *has order* n *modulo* m. *Then* a^t *also has order* n *if and only if* $\gcd(t, n) = 1$ *i.e.* $ord_m a^t = n \iff \gcd(t, n) = 1$.

Proof. From Theorem 8.2.3, we have $ord_m a^t = \frac{n}{\gcd(t,n)}$. Then $ord_m a^t = n$ if and only if $\gcd(t, n) = 1$. ☐

Example 8.2.2. The following example will exemplify Theorem 8.2.3. Let us choose $a = 4$ and $m = 13$. Then $4^6 \equiv 1(\bmod 13)$. Thus $ord_{13} 4 = 6$. Now $ord_{13} 4^9 = \dfrac{6}{\gcd(6, 9)} = 2$. In fact $4^{18} = (4^6)^3 \equiv 1(\bmod 13)$.

In Corollary 8.2.1, we have seen that order of integer modulo m must divide $\phi(m)$, provided a and m are prime to each other. If the order of integer modulo m becomes exactly $\phi(m)$, then a is called primitive root of m.

Definition 8.2.2. *For an arbitrary integer* a *relatively prime to a positive integer* m *with* $ord_m a = \phi(m)$ *then,* a *is called the primitive root of* m.

In fact, the above definition can be written as $a^{\phi(m)} \equiv 1(\bmod m)$ where $\gcd(a, m) = 1$. For instance if we choose $a = 5$ and $m = 7$ then, $\phi(7) = 6$ as 7 is prime and we see that $5^6 \equiv 1(\bmod 7)$ verifying 5 as a primitive root of 7. Also there are some cases where we cannot find primitive roots. For example if we choose $a = 7$ and $m = 6$ then, the integers less than 6 and prime to 6 are $1, 5$. Thus, $\phi(6) = 2$ and also $7 \equiv 1(\bmod 6)$ but $7^2 \not\equiv 1(\bmod 6)$. So in this case 7 is not a primitive root modulo 6. Our next theorem is going to exhibit an important property of primitive roots.

Theorem 8.2.4. *If* a *and* $m(> 0)$ *are relatively prime and if* a *is primitive root of modulo* m, *then the integers* $a^1, a^2, \cdots a^{\phi(m)}$ *forms a reduced residue system modulo* m.

Proof. Its suffices to prove, all of the integers $a^1, a^2, \cdots a^{\phi(m)}$ are incongruent modulo m. If not, let $a^i \equiv a^j(\bmod m)$ for $1 \leq i < j \leq \phi(m)$. Thereby using Theorem 8.2.2, we can say that $i \equiv j(\bmod \phi(m))$. But this is possible only if $i = j$, which proves that $a^1, a^2, \cdots a^{\phi(m)}$ are incongruent modulo m. Hence $a^1, a^2, \cdots a^{\phi(m)}$ forms a reduced residue system of modulo m. ☐

The following corollary deals with finding the number of primitive roots:

Corollary 8.2.3. *If an integer* $m(> 0)$ *has primitive root then, the number is exactly* $\phi(\phi(m))$.

Proof. Let a be a primitive root modulo m. Then from Theorem 8.2.4, all the integers $a^1, a^2, \cdots a^{\phi(m)}$ forms a reduced residue system modulo m. Again using

Corollary 8.2.2, we can assert that a^t is a primitive root modulo m if and only if $\gcd(t, \phi(m)) = 1$. As there are $\phi(\phi(m))$ such integers then the number of primitive roots are exactly $\phi(\phi(m))$. ☐

Example 8.2.3. Let us choose $a = 2$ and $m = 11$. Then the integers less than 11 and prime to 11 are $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. In fact $\phi(11) = 10$. Its obvious that $2^{10} \equiv 1(\text{mod } 11)$. Thus 2 is a primitive root modulo 11. Now from the above corollary, we can say there are exactly $\phi(\phi(10)) = 4$ primitive roots as the integers less than 10 and prime to 10 are $1, 3, 7, 9$. Now $2^3 = 8 \equiv 8(\text{mod } 11)$, $2^7 = 128 \equiv 7(\text{mod } 11)$, $2^9 = 512 \equiv 6(\text{mod } 11)$. So here the primitive roots of 11 are $2, 6, 7, 8$.

8.3 Worked out Exercises

Problem 8.3.1. *Find the order of the integers* $2, 3,$ *&* 5 *modulo* 19*.*

Solution 8.3.1. *Here* $\phi(19) = 18$*. Therefore the divisors of* 18 *are* $1, 2, 3, 6, 9, 18$*. Under modulo* 19*,*

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^6 \equiv 7,\ 2^9 \equiv 18,\ 2^{18} \equiv 1$$

imply order of 2 *is* 18*. By similar reasoning,*

$$3^2 \equiv 9,\ 3^3 \equiv 8,\ 3^6 \equiv 7,\ 3^9 \equiv 18,\ 3^{18} \equiv 1$$

generates order of 3 *to be* 18 *and*

$$5^2 \equiv 6,\ 5^3 \equiv 11,\ 5^6 \equiv 7,\ 5^9 \equiv 1$$

produces order of 5 *to be* 9*.*

Problem 8.3.2. *If k is a positive integer and a is an integer relatively prime to k such that order of a modulo k is $k - 1$ then, show that k is prime.*

Solution 8.3.2. *An appeal to Euler's theorem yields* $a^{k-1} \equiv 1(\text{mod } k)$ *and* $a^{\phi(k)} \equiv 1(\text{mod } k)$*. If* $\phi(k) < k - 1$*, then this leads to a contradiction. Hence* $\phi(k) = k - 1$*. If k were composite, then it would have a divisor d with* $1 < d < k$*. Furthermore, k is a divisor of itself and this implies* $\phi(k) \leq (k - 2)$*. But* $\phi(k) = k - 1$ *shows that k is not composite and hence a prime.*

Problem 8.3.3. *Assume that the order of a modulo n is h and the order of b modulo n is k. Show that the order of ab modulo n divides hk; in particular, if* $\gcd(h, k) = 1$ *then ab has order hk.*

Solution 8.3.3. *We note that*

$$\begin{aligned} a^h &\equiv 1(\mod n) \Rightarrow a^{hk} \equiv 1(\mod n), \\ b^k &\equiv 1(\mod n) \Rightarrow b^{kh} \equiv 1(\mod n). \\ \therefore (ab)^{hk} &= a^{hk}b^{hk} \equiv 1(\mod n). \end{aligned}$$

Thus by virtue of Theorem 8.2.1, order of ab *divides* hk. *Next suppose* $\gcd(h,k) = 1$. *Let* $h = p_1^{h_1}p_2^{h_2}\cdots p_r^{h_r}$ & $k = q_1^{k_1}q_2^{k_2}\cdots q_s^{k_s}$. *Here* $q_j \neq p_j$ *as* $\gcd(h,k) = 1$. *Let* ω *be the order of* ab. *Then* $\omega \big| hk$. *So*

$$\omega = p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}q_1^{m_1}q_2^{m_2}\cdots q_s^{m_s},$$

where $0 \leq l_i \leq h_i$, $0 \leq m_i \leq k_i$. *Let* $\omega = h_x k_y$, $h_x = p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}$, $k_y = q_1^{m_1}q_2^{m_2}\cdots q_s^{m_s}$. *Thus* $h_x|h$, $k_y|k$. *Let* $h = \tilde{h}h_x$ & $k = \tilde{k}k_y$.

$$\therefore\ (ab)^{h_x k_y} = a^{h_x k_y}b^{h_x k_y} \equiv 1(\mod n).$$

$$\therefore\ (a^{h_x k_y}b^{h_x k_y})^{\tilde{h}} \equiv 1(\mod n). \tag{8.3.1}$$

$$\begin{aligned} \text{But } (a^{h_x k_y}b^{h_x k_y})^{\tilde{h}} &= a^{\tilde{h}h_x k_y}b^{\tilde{h}h_x k_y} \\ &= (a^h)^{k_y}(b^h)^{k_y} \equiv (b^h)^{k_y}(\mod n), \text{ as } a^h \equiv 1(\mod n). \end{aligned} \tag{8.3.2}$$

(8.3.1) and (8.3.2) together imply $(b^h)^{k_y} \equiv 1(\mathrm{mod}\ n)$. *Since order of* b *is* k, *therefore we get* $k|hk_y$ *(refer to Theorem 8.2.1). Since* $\gcd(h,k) = 1$, *therefore* $k|k_y$. *Hence* $k|k_y$, $k_y|k \Rightarrow k = k_y$. *Similarly,* $h = h_x$. *Finally,* $\omega = hk$. *So* $\gcd(h,k) = 1 \Rightarrow$ *order of* $ab = hk$.

Problem 8.3.4. *Prove that the odd prime divisors of the integer* $n^4 + 1$ *are of the form* $8k + 1$.

Solution 8.3.4. *Assume* $p\big|(n^4 + 1)$. *Therefore* $n^4 \equiv -1(\mathrm{mod}\ p) \Rightarrow n^8 \equiv 1(\mathrm{mod}\ p)$. *Here* $\gcd(n,p) = 1$, *for if* $n = kp$ $(k \in \mathbb{Z}) \Rightarrow n^4 = (kp)^4 \Rightarrow p|n^4$. *This combines with* $p|(n^4 + 1)$ *gives* $p|1$, *which is impossible. Let* r *be the order of* n *modulo* p. *Therefore* $r|8$ *[refer to Theorem 8.2.1]. Thus,* $r = 1, 2, 4, 8$. *Here order of* n *can not be* 1, *for* $n \equiv 1 \Rightarrow n^4 \equiv 1$. *Similarly, order of* n *can not be* 2 *and* 4*(Why!). Hence order of* n *modulo* p *must be* 8. *Therefore* $8|\phi(p) \Rightarrow 8|(p-1) \Rightarrow p = 8k+1$ *where* $k \in \mathbb{Z}$.

Problem 8.3.5. *Prove that if* p *and* q *are odd primes and* $q\big|(a^p - 1)$, *then either* $q|(a-1)$ *or else* $q = 2kp + 1$ *for some integer* k.

Solution 8.3.5. *Our first claim is* $\gcd(a,q) = 1$. *For if, let* $\gcd(a,q) = d(>1)$. *Then* $d|q$ & $q\big|(a^p - 1)$ *together yields* $d\big|(a^p - 1)$. *Also* $d|a$ *implies* $d|1$, *a* *contradiction. Hence our first claim is fulfilled. Now* $q\big|(a^p - 1) \Rightarrow a^p \equiv 1(\bmod q)$. *Let* r *be the order of* a *modulo* q. *Then* $r|p$ *[refer to Theorem 8.2.1]. Moreover* p *being prime shows* $r = 1$ *or* p. *If* $r = 1$, *then* $a \equiv 1(\bmod q) \Rightarrow q|(a-1)$. *If* $r = p$, *then* $p|\phi(q)$ *(Explain Why!). But* $\phi(q) = q - 1$. *Therefore* $p|(q-1) \Rightarrow p\tilde{k} = q - 1,\ \tilde{k} \in \mathbb{Z}$. *But* q *being odd implies* $q - 1$ *is even. Since* p *is odd,* $\tilde{k}$ *must be even, so* $\tilde{k} = 2k$ *for some* $k \in \mathbb{Z}$. *Therefore* $p(2k) = q - 1,\ q = 2pk + 1$ *for some* k.

Problem 8.3.6. *Verify that* 2 *is a primitive root of* 19, *but not of* 17.

Solution 8.3.6. *Here,*

$$\begin{aligned}\phi(19) = 18, \quad 2^6 &= 64 \equiv 7(\bmod 9)\\ 7^2 &= 49 \equiv 11(\bmod 19)\\ 7^3 &\equiv 77 = 4\cdot 19 + 1 \equiv 1(\bmod 19)\\ 2^{18} &= (2^6)^3 \equiv 7^3 \equiv 1(\bmod 19).\end{aligned}$$

Therefore $2^{18} = 2^{\phi(19)} \equiv 1(\bmod 19)$. *Suppose order of* 2 *modulo* $19 = r(< 18)$. *This implies* $r|18$. *So* $r = \{1, 2, 3, 6, 9\}$. *Now,*

$$\begin{aligned}2^1 &\not\equiv 1(\bmod 19) \Rightarrow r \neq 1.\\ 2^2 &\not\equiv 1(\bmod 19) \Rightarrow r \neq 2.\\ 2^3 &\not\equiv 1(\bmod 19) \Rightarrow r \neq 3.\\ 2^6 \equiv 7 &\not\equiv 1(\bmod 19) \Rightarrow r \neq 6.\\ 2^9 \equiv 8\cdot 7 = 56 &\equiv 18(\bmod 19) \Rightarrow r \neq 9.\end{aligned}$$

So $\phi(19) = 18$ *is the smallest integer* r *for which* $2^r \equiv 1(\bmod 19)$. *Hence* 2 *is a primitive root of* 19.

Next for 17, $\phi(17) = 16$. *Let* r *be the order of* 2. *Therefore* $r \in \{1, 2, 8, 16\}$. *Here* $r \neq 1, 2, 4$ *(Verify!). Now*

$$\begin{aligned}2^8 &= 15\cdot 17 + 1 \equiv 1(\bmod 17).\\ \therefore\ 2^8 &\equiv 1(\bmod 17).\end{aligned}$$

So order of $2 \bmod 17$ *is* 8 *and not* 16. *Hence* 2 *is not a primitive root of* 17.

Problem 8.3.7. *Let* r *be a primitive root of the integer* n. *Prove that* r^k *is a primitive root of* n *if and only if* $\gcd(k, \phi(n)) = 1$.

Solution 8.3.7. *Since* r *has order* $\phi(n)$ *modulo* n, *by virtue of Theorem 8.2.3,* r^k *has order* $\dfrac{\phi(n)}{\gcd(k, \phi(n))}$ *modulo* n. *Now if* $\gcd(k, \phi(n)) = 1$, *then* r^k *has order* $\phi(n)$ *implies* r^k *is a primitive root of* n.

Conversely, suppose r^k *is a primitive root of* n*. Then,* r^k *has order* $\phi(n)$ *modulo* n*. From above,* $\phi(n) = \frac{\phi(n)}{\gcd(k,\phi(n))} \Rightarrow \gcd(k, \phi(n)) = 1$.

Problem 8.3.8. *Prove that if* p *and* $q > 3$ *are both odd primes and* $q|R_p$*, then* $q = 2kp + 1$ *for some integer* k*.*

Solution 8.3.8. *Here,* $R_p = \dfrac{10^p - 1}{q}$*. If* $q|R_p$ *then for some* r*,* $qr = \dfrac{10^p - 1}{q} \Rightarrow q(qr) = 10^p - 1$*. This shows* $q|10^p - 1$ *implying* $q|(10-1)$ *or* $q = 2kp+1$ *for some* k*[refer to worked out Problem 8.3.5]. Since* $q > 3$*, then* $q \nmid (10 - 1)$*. Therefore* $q = 2kp + 1$ *for some integer* k*.*

Problem 8.3.9. *Prove that* a *is a primitive root modulo odd prime* p *if and only if* a *is an integer with* $\gcd(a, p) = 1$ *such that*

$$a^{\frac{(p-1)}{q}} \not\equiv 1(\mod p)$$

for all prime divisors q *of* $p - 1$*.*

Solution 8.3.9. *Let* a *be a primitive root modulo* p*. Then the order of* a *modulo* p *is* $\phi(p) = p - 1$*. Thus for any prime divisor* q *of* $p - 1$ *we can assert that*

$$a^{\frac{(p-1)}{q}} \not\equiv 1(\mod p).$$

In anticipation of a contrapositive argument, let a *be not a primitive root of* p*. Then there exists an integer* $t < p - 1$ *with* $a^t \equiv 1(\mod p)$*. Now from Corollary 8.2.1, we can say that* t *divides* $p - 1$*. This implies that* $p - 1 = st$ *for some integer* $s(> 1)$*. Then we have* $\frac{p-1}{s} = t$*. Let* q *be a prime divisor of* s*. This shows that* $\frac{p-1}{q} = t \cdot (\frac{s}{q})$*. From this we get,*

$$a^{\frac{(p-1)}{q}} = a^{t(\frac{s}{q})} = (a^t)^{\frac{s}{q}} \equiv 1(\mod p).$$

This finishes the proof of the converse part.

Problem 8.3.10. *Prove that if* a *is a primitive root modulo* m*, then* $\overline{a}$ *is also primitive root modulo* m*, where* $\overline{a}$ *is an inverse of* a *modulo* m*.*

Solution 8.3.10. *Let* a *be a primitive root modulo* m*, then we have* $a^{\phi(m)} \equiv 1(\mod m)$*. Let the order of* $\overline{a}$ *modulo* m *be* k*. Then by virtue of Corollary 8.2.1 we get* $k|\phi(m)$*. Since* $\overline{a}$ *is inverse of* a *modulo* m *then,*

$$\begin{aligned} a\overline{a} &\equiv 1(\mod m) \\ \Rightarrow (a\overline{a})^k &\equiv 1(\mod m) \\ \Rightarrow a^k(\overline{a})^k &\equiv 1(\mod m) \\ \Rightarrow a^k &\equiv 1(\mod m). \end{aligned}$$

This shows that $\phi(m)|k$*. Combining* $k|\phi(m)$ *and* $\phi(m)|k$ *yields* $k = \phi(m)$*. This proves that* $\overline{a}$ *is also primitive root modulo* m*.*

8.4 Primitive Roots for Primes

In the foregoing section we have dealt with an important concept, known as primitive roots. In the present section we will study whether every prime has a primitive root or not. To proceed further, the concept of polynomial congruence will act as an important tool. The definition of polynomial congruence is as follows:

Definition 8.4.1. *Let* $f(x)$ *be a polynomial with integral coefficients, then the expression* $f(x) \equiv 0(\mod m)$ *is known to be polynomial congruence modulo* m*.*

Here in polynomial congruence an integer a is a root of $f(x)$ modulo m if $f(a) \equiv 0(\mod m)$. Also if a is a root of $f(x)$ modulo m then it is obvious that every integer which are congruent to a modulo m is also a root of $f(x) \equiv 0(\mod m)$.

For instance, let $f(x) = x^2 + 2x + 4$ has two incongruent roots modulo 6 and they are $x \equiv 2(\mod 6)$, $x \equiv -4(\mod 6)$. If we choose $g(x) = x^2 + 2$ then it has no roots modulo 6. The next theorem deals with roots of a polynomial modulo p, where p is prime.

Theorem 8.4.1. *(Lagranges): Let* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ *and* $p \nmid a_n$ $(n \geq 1)$*, where* p *is prime then the polynomial congruence* $f(x) \equiv 0(\mod p)$ *has at most* n *incongruent solutions modulo* p*.*

Proof. Let us apply the principle of Mathematical induction on n, degree of $f(x)$. If $n = 1$ then $f(x) = a_1x + a_0$. Since $p \nmid a_1$ then $\gcd(a_1, p) = 1$, thus the congruence equation $a_1x \equiv a_0(\mod p)$ has unique solution[refer to Corollary 4.4.1]. Thus the result is true for $n = 1$.

Suppose the statement is true for all polynomials whose degree is $k(> 1)$. Let the degree of $f(x)$ be $k + 1$, whose one of the roots being chosen as α. Then we have, $f(x) = (x - \alpha)g(x) + r$, where the degree of $g(x)$ is k with integral coefficients. Also, r is constant. Since α is a root of $f(x)$ then, $f(\alpha) = (\alpha - \alpha)g(\alpha) + r \equiv 0(\mod p)$. So we can write, $f(x) = (x - \alpha)g(x)(\mod p)$. Now as the degree of $g(x)$ is k then p does not divide the leading coefficient of $g(x)$, otherwise p will divide the leading coefficient of $f(x)$ whose degree is $k + 1$. If β be another root of $f(x)$ then, $f(\beta) \equiv 0(\mod p) \Rightarrow (\beta - \alpha)g(\beta) \equiv 0(\mod p)$. As α, β are different roots under congruence modulo p, then we have $g(\beta) \equiv 0(\mod p)$. As the degree of $g(x)$ is k, by induction hypothesis, at most k numbers of β are possible.

Therefore $f(x) \equiv 0(\mod p)$ has at most $k + 1$ incongruent solutions modulo p. Thus the statement is true for $n = k + 1$ and hence it is true for all integers $n(\geq 1)$. □

This result leads to an observation that is useful in certain situations; namely,

Corollary 8.4.1. *If p is prime and q divides $p-1$, then the congruence equation, $x^q - 1 \equiv 0(\bmod\ p)$ has exactly q incongruent solutions.*

Proof. Here $q|(p-1)$ implies $p-1 = qk$ for some integer k. Then,

$$\begin{aligned} x^{p-1} - 1 &= (x^q - 1)(x^{q(k-1)} + x^{q(k-2)} + \cdots + x^q + 1) \\ &= (x^q - 1)R(x). \end{aligned}$$

Here $R(x) = x^{q(k-1)} + x^{q(k-2)} + \cdots + x^q + 1$ whose degree is $q(k-1) = qk - q = (p-1) - q$. Applying Theorem 8.4.1 we can say that $R(x)$ has at most $(p-1) - q$ incongruent roots. Also from Fermat's little theorem, $x^{p-1} - 1 \equiv 0(\bmod\ p)$ has $p-1$ incongruent roots under modulo p. Now let $x = c$ be a solution of $x^{p-1} - 1 \equiv 0(\bmod\ p)$ but not a solution of $R(x) \equiv 0(\bmod\ p)$. Then $x = c$ must be the solution of $x^q - 1 \equiv 0(\bmod\ p)$. So Theorem 8.4.1 yields the number of incongruent solutions of $x^q - 1 \equiv 0(\bmod\ p)$ is exactly $(p-1) - (p-1) + q = q$. □

Now we are in a stage to assert that for any prime p and any divisor q of $p-1$, the congruence equation whose degree is q has exactly q different solutions under modulo p. Our next theorem focuses on the number of integers having a given order under modulo p.

Theorem 8.4.2. *Let p be prime and d a positive divisor of $p-1$. Then the number of incongruent integers of order d modulo p is $\phi(d)$.*

Proof. Let $d|(p-1)$ and $\chi(d)$ be the number of positive integers having order d modulo p which are less than p. Since every integer lying between 1 and $p-1$ has order d for some $d|(p-1)$, it follows

$$p - 1 = \sum_{d|(p-1)} \chi(d).$$

Again from Theorem 7.6.1 we observe that,

$$p - 1 = \sum_{d|p-1} \phi(d).$$

Combining the last two equations, we obtain

$$\sum_{d|(p-1)} \chi(d) = \sum_{d|(p-1)} \phi(d). \tag{8.4.1}$$

Claim: $d|(p-1) \Rightarrow \chi(d) \le \phi(d)$. From (8.4.1) it follows that $\chi(d) = \phi(d)$. If $\chi(d) = 0$ then we are done. Let us choose $\chi(d) > 0$, which shows that there exists an integer n of order d. Then there exists d number of integers $n, n^2, n^3, \cdots, n^d$ which are incongruent modulo p. Also, these integers satisfy the equation $x^d \equiv 1(\bmod p)$ because, $(n^k)^d = (n^d)^k \equiv 1(\bmod p)$ where $k \in \{1, 2, \cdots, d\}$. However the Corollary 8.2.2 signifies that any power k of a is of the order d modulo p provided $\gcd(k, p) = 1$. Finally, we conclude that k is no one but $\phi(d)$ and also $\chi(d) = \phi(d)$. So the number of incongruent integers having order d modulo p is $\phi(d)$. This proves the theorem. ☐

If we substitute $d = p - 1$ then we arrive at the following corollary:

Corollary 8.4.2. *Every prime has a primitive root.*

Proof. In the above theorem, taking $d = p - 1$, p being a prime, we can say that there are $\phi(p-1)$ incongruent integers of order $p-1$ modulo p. Using the definition of primitive root, for any integer a relatively prime to p, the order of a becomes $d = p - 1 = \phi(d)$ modulo p implies a is a primitive root. ☐

Remark 8.4.1. *Using Corollary 8.2.3, for any prime p which has a primitive root, the number of primitive roots are* $\phi(\phi(p)) = \phi(p-1)$.

Finally, the following example illustrates the above results:

Example 8.4.1. *Choose* $p = 29$. *Then* $d = 4$ *is a divisor of* $p - 1 = 28$. *So the number of integers incongruent modulo* 31 *of order* 4 *is* $\phi(4) = 2$. *Also, there are* $\phi(\phi(29)) = \phi(28) = 14$ *number of primitive roots. Taking* $n = 12$, *shows* $12^4 \equiv 1(\bmod 29)$ *(Verify!), satisfies* $x^4 - 1 \equiv 0(\bmod 29)$. *So the number of integers of the form* 12^k *where* $1 \le k \le 28$, *are relatively prime to and less than* 29. *Now the order of* 12^k *is* $\dfrac{28}{\gcd(k, 28)} = 4$, *if* $k = 7, 21$.

Finally we need to evaluate 12^7 *and* 12^{21} *modulo* 29. *In fact,*

$$12^7 \equiv 17(\bmod 29)$$
$$12^{21} \equiv 12(\bmod 29).$$

Thus 12 *and* 17 *are the only integers of order* 4 *modulo* 29. *Again if we choose* $n = 2$ *and* $d = p - 1 = 28$ *then we have* $2^{28} \equiv 1(\bmod 29)$. *This shows that* 2 *is the primitive root modulo* 29.

The concluding part of the section deals with the following table which lists the smallest positive primitive root for each prime below 200.

Prime	Least Positive Primitive Root	Prime	Least Positive Primitive Root
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

Table 8.1: Primitive root for Primes

8.5 Worked out Exercises

Problem 8.5.1. *Prove for an odd prime p, the only incongruent solutions of* $x^2 \equiv 1 (\bmod\ p)$ *are* 1 *and* $p-1$.

Solution 8.5.1. *Since p is odd prime therefore,* $2\big|(p-1)$. *Hence with reference to Corollary 8.4.1, the congruence equation has exactly* 2 *incongruent solutions. Clearly,* 1 *is a solution as* $1 \equiv 1 (\bmod\ p)$. *Now* $p-1$ *is also a solution as* $(p-1)^2 \equiv 1 (\bmod\ p)$. *Therefore* 1 *and* $p-1$ *are solutions and they are incongruent modulo p.*

Problem 8.5.2. *Find all the positive integers less than* 43 *having order* 6 *modulo* 43, *provided* 3 *is a primitive root of* 43.

Solution 8.5.2. *By virtue of Theorem 8.2.2,* $3^k (1 \leq k \leq 42)$ *are incongruent. Thus, all integers less than* 43 *are congruent to* 3^k *having the order* $\dfrac{42}{\gcd(k, 42)}$ *modulo* 43*[refer to Theorem 8.2.3]. Now*

$$\frac{42}{\gcd(k, 42)} = 6 \Rightarrow \gcd(k, 42) = 7 \Rightarrow k = 7,\ 35.$$

Thus, $3^7, 3^{35}$ *have order* 6 *modulo* 43. *Here,*

$$\begin{aligned}
&3^3 = 27, 3^4 = 81 \equiv -5(\bmod 43),\\
\therefore\ &3^7 \equiv -135 \equiv -135 + 3\cdot 43 \equiv 37 \equiv -6(\bmod 43).\\
&3^7 \cdot 3^7 \equiv (-6)(-6) \equiv 36 \equiv (-7)(\bmod 43),\\
&3^{18} \equiv (-7)(-5) \equiv 35 \equiv (-8)(\bmod 43).\\
&3^{32} \equiv 3^{14} \cdot 3^{18} \equiv (-7)(-8) \equiv 56 \equiv 13(\bmod 43).\\
&3^{33} \equiv 39 \equiv -4(\bmod 43),\\
\therefore\ &3^{35} \equiv 9(-4) = -36 \equiv 7(\bmod 43).
\end{aligned}$$

Hence $7(\equiv 3^{35})$, $37(\equiv 3^7)$ *have order* 6 *modulo* 43.

Problem 8.5.3. *Considering r as a primitive root of the odd prime p, prove the following:*

1. *The congruence* $r^{\frac{p-1}{2}} \equiv -1 (\bmod\ p)$ *holds.*
2. *If* r_1 *is any other primitive root of p, then* rr_1 *is not a primitive root of p.*
3. *If for the integer* r', $rr' \equiv 1 (\bmod\ p)$ *holds then* r' *is also a primitive root of p.*

Solution 8.5.3. *1. From Fermat's theorem, we have* $r^{p-1} \equiv 1(\bmod p)$*. As* $\frac{p-1}{2} \in \mathbb{Z}$*, therefore* $r^{\frac{p-1}{2}}$ *exists.*

$$\therefore\ r^{p-1} - 1 \equiv 0(\bmod p) \Rightarrow (r^{\frac{p-1}{2}} - 1)(r^{\frac{p-1}{2}} + 1) \equiv 0(\bmod p).$$

If $(r^{\frac{p-1}{2}} - 1) \equiv 0(\bmod p)$*, then* r *fails to have order* $p-1$*(Why!).*

$$\therefore\ (r^{\frac{p-1}{2}} + 1) \equiv 0(\bmod p) \Rightarrow r^{\frac{p-1}{2}} \equiv -1(\bmod p).$$

2. On the contrary, if rr_1 *would have been a primitive root of* p *then its order would be* $p-1$*. By virtue of (1),*

$$\begin{aligned} & r^{\frac{p-1}{2}} \equiv -1(\bmod p), \quad \& \quad r_1^{\frac{p-1}{2}} \equiv -1(\bmod p), \\ \Rightarrow\ & r^{\frac{p-1}{2}} r_1^{\frac{p-1}{2}} \equiv (-1)(-1)(\bmod p), \\ \Rightarrow\ & (rr_1)^{\frac{p-1}{2}} \equiv 1(\bmod p). \end{aligned}$$

A contradiction to our hypothesis(Why!). Hence the statement follows.

3. Let us assume $1 \leq r' \leq p-1$*. For if* $r' = p$ *then,* $r' \equiv 0(\bmod p)$*. If* $r' > p$ *then, by division algorithm we can write* $r' = qp + s$ *for some integers* q *and* s *with* $0 \leq s < p-1$*. This implies* $r' \equiv s(\bmod p)$ *and both* r' *and* s *have same order. This follows that* $\gcd(r', p) = 1$*. Now consider* $(r')^k$ *with* $1 \leq k \leq p-1$*. If* $k < p-1$ *and* $(r')^k \equiv 1(\bmod p)$ *then,* $1 = 1^k \equiv (rr')^k = r^k(r')^k \equiv r^k(\bmod p)$*. This contradicts the fact that* r *is a primitive root modulo* p*. Therefore* $1 = 1^{p-1} \equiv (rr')^{p-1} = r^{p-1}(r')^{p-1} \equiv r^k(\bmod p)$*. Now* $(r')^k \not\equiv 1(\bmod p)(1 \leq k < p-1)$ *and* $\gcd(r', p) = 1$ *together implies that* r' *is a primitive root of* p*.*

Problem 8.5.4. *For a prime* $p > 3$*, prove that the primitive roots of* p *occur in incongruent pairs* $r, \tilde{r}$ *where* $r\tilde{r} = 1(\bmod p)$*.*

Solution 8.5.4. *Referring to Theorem 7.2.4, for* $n > 2$*,* $\phi(n)$ *is an even integer so that* $\phi(n) \geq 2$*. Let* r *be one primitive root of* p*. Then* $r, r^2, \ldots, r^{p-1}$ *are congruent to* $1, 2, 3, \ldots, p-1$ *in some order and so* $r, r^2, \ldots, r^{p-1}$ *are incongruent[refer to Theorem 8.2.4]. Since* $p > 3$*, there are at least three members in the list. Let* $\tilde{r} = r^{p-2}$*. Then* r *and* $\tilde{r}$ *are incongruent and* $r\tilde{r} = r^{p-1} \equiv 1(\bmod p)$*. So* $\tilde{r}$ *is another primitive root(refer last problem), thereby it follows that if* r *is a primitive root of* $p(> 3)$ $\exists$ *another primitive root* $\tilde{r}$ *incongruent to* r *such that* $r\tilde{r} = 1(\bmod p)$*.*

Problem 8.5.5. *Use the fact that each prime* p *has a primitive root to give a different proof of Wilson's theorem.*

Solution 8.5.5. *Let* r *be a primitive root of* p. *Now,* $1, 2, 3, \ldots, p-1$ *are the positive integers relatively prime to* p. *Also,* $\phi(p) = p-1$. *Then, by virtue of Theorem 8.2.4,* $r, r^2, \ldots, r^{p-1}$ *are congruent modulo* p *to* $1, 2, 3, \ldots, p-1$ *in same order.*

$$\begin{aligned}
&\therefore r \cdot r^2 \cdots r^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)(\bmod p)\\
&\Rightarrow r^{1+2+3+\ldots+(p-1)} \equiv (p-1)!(\bmod p)\\
&\Rightarrow r^{\frac{p(p-1)}{2}} \equiv (p-1)!(\bmod p)\\
&\Rightarrow (r^{p-1})^p \equiv [(p-1)!]^2(\bmod p). \qquad (8.5.1)
\end{aligned}$$

Since r *is a primitive root of* p, *therefore* $r^{p-1} \equiv 1(\bmod p)$. *So* $(r^{p-1})^p \equiv 1(\bmod p)$. *Thus from equation(8.5.1), we obtain*

$$\begin{aligned}
&[(p-1)!]^2 \equiv 1(\bmod p)\\
\Rightarrow\ &[(p-1)!]^2 - 1 \equiv 0(\bmod p)\\
\Rightarrow\ &[(p-1)!+1][(p-1)!-1] \equiv 0(\bmod p).
\end{aligned}$$

If $(p-1)! - 1 \equiv 0(\bmod p)$, *then* $r^{\frac{(p-1)p}{2}} \equiv (p-1)! \equiv 1(\bmod p)$. *But* $r^{p-1} \equiv 1(\bmod p) \Rightarrow r^p \equiv r(\bmod p)$. *Therefore* $r^{\frac{(p-1)p}{2}} = (r^p)^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \equiv 1(\bmod p)$. *Thereby contradicts the fact that the order of* $r = p-1$, *as* $\dfrac{p-1}{2} < (p-1)$. *Hence* $(p-1)! + 1 \equiv 0(\bmod p) \Rightarrow (p-1)! \equiv (-1)(\bmod p)$.

Problem 8.5.6. *If* p *is a prime, show that the product of the* $\phi(p-1)$ *primitive roots of* p *is congruent modulo* p *to* $(-1)^{\phi(p-1)}$.

Solution 8.5.6. *Since* r *is a primitive root of* p, *therefore* $r, r^2, \ldots, r^{p-1}$ *are congruent modulo* p *to* $1, 2, 3, \ldots, p-1$ *in some order[refer to Theorem 8.2.4]. If* s *be any other primitive root of* p, *it must be congruent to one of* $1, 2, 3, \ldots, p-1$. *Therefore* s *is congruent to one of* $r, r^2, \ldots, r^{p-1}$. *Hence all primitive roots of* p *are of the form* r^k, *where* $1 \leq k \leq p-1$. *Since* $\gcd(k, p-1) = 1$, *therefore we have* $k \neq p-1$. *So* k *must be of the form* $1 \leq k < p-1$. *Let us denote these* $\phi(p-1)$ *integers as* $k_1, k_2, \ldots, k_{\phi(p-1)}$, $1 \leq k_i < p-1$. *Thus, the product of these primitive roots is*

$$r^{k_1} r^{k_2} \cdots r^{k_{\phi(p-1)}} = r^{k_1+k_2+\ldots+k_{\phi(p-1)}}.$$

Now Theorem 7.6.2 yields

$$k_1 + k_2 + \ldots + k_{\phi(p-1)} = \frac{1}{2}(p-1)\phi(p-1).$$

$$\therefore\ r^{k_1+k_2+\ldots+k_{\phi(p-1)}} = r^{\frac{1}{2}(p-1)\phi(p-1)}.$$

For $p > 2$, $\phi(p-1)$ *is even[refer to Theorem 7.2.4]. So* $2|\phi(p-1)$.

$$\therefore\ r^{\frac{1}{2}(p-1)\phi(p-1)} = \left(r^{(p-1)}\right)^{\frac{1}{2}\phi(p-1)},$$

$$\equiv (1)^{\frac{1}{2}\phi(p-1)} \equiv 1(\mod p),\ \because,\ \frac{1}{2}\phi(p-1) \geq 1,\ \textit{for}\ p > 2.$$

Since $\phi(p-1)$ *is even,* $(-1)^{\phi(p-1)} = 1$. *This shows that,*

$$r^{k_1+k_2+\ldots+k_{\phi(p-1)}} \equiv (-1)^{\phi(p-1)}(\mod p).$$

For $p = 2$, *the only primitive root is* 1, $\phi(2) = 1$ *and so,*

$$r^{k_1+k_2+\ldots+k_{\phi(p-1)}} = 1 \equiv (-1)(\mod 2),\ \because,\ 1 \equiv (-1)(\mod 2).$$

Hence the formula holds for $p = 2$.

Problem 8.5.7. *Show that if* p *is a prime and* $p = 2q+1$, *where* q *is an odd prime and* a *is a positive integer with* $1 < a < p-1$, *then* $p - a^2$ *is a primitive root modulo* p.

Solution 8.5.7. *Since* p *is a prime, therefore* $\phi(p) = p - 1 = 2q$. *Now the possible orders of* $p - a^2$ *are* $1, 2, q$ *and* $2q$.

If $p - a^2$ *has the order* 2, *then we get*

$$(p-a^2)^2 = p^2 - 2pa^2 + a^4 \equiv a^4(\mod p).$$

Here $a^2 \equiv 1(\mathrm{mod}\ p)$, *as* a *can not be of order* 4. *Thus we have* $a \equiv \pm 1(\mathrm{mod}\ p)$. *But this is not possible, because* $1 < a < p-1$. *This shows* $p - a^2$ *does not posses order* 2.

If $p - a^2$ *has order* q, *then using binomial theorem we get*

$$(p-a^2)^q \equiv -(a^{2q}) \equiv -1(\mod p).$$

Again, this proves $p - a^2$ *does not posses order* q.

Hence $(p - a^2)$ *has the order* $2q$ *and* $(p - a^2)$ *becomes a primitive root modulo* p.

Problem 8.5.8. *Let* r *be a primitive root of the prime* p *with* $p \equiv 1(\mod 4)$. *Show that* $-r$ *is also a primitive root.*

Solution 8.5.8. *Let* r *be a primitive root modulo* p *where* $p \equiv 1(\mathrm{mod}\ 4)$. *Let* t *be the order of* $-r$ *modulo* p. *Thus, from Corollary 8.2.1 we have* $t|(p-1)$. *This shows* $p - 1 = kt$ *for some integer* k. *Here we need to show* $k = 1$. *For that, let us suppose* $k > 1$. *Two cases arise:*

Case-I: *If k is odd, then $t = \frac{p-1}{k}$ is even. This gives $(-r)^t = r^t \equiv 1(\mathrm{mod}\ p)$, which contradicts the fact that r is a primitive root modulo p.*

Case-II: *If k is even, then $(-r)^t = (-r)^{\frac{p-1}{k}} \equiv 1(\mathrm{mod}\ p)$. As k is even, then $\frac{p-1}{k}\Big|\frac{p-1}{2}$ gives $(-r)^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$. Here $\frac{p-1}{2}$ is even as, $p \equiv 1(\mathrm{mod}\ 4)$. Hence*

$$(-r)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}(r)^{\frac{p-1}{2}} = r^{\frac{p-1}{2}} \equiv 1(\ \mathrm{mod}\ p).$$

Again we arrive at a contradiction(Why!). Thus the only possibility remains $k = 1$. This shows $-r$ is a primitive root modulo p.

8.6 Existence of Primitive Roots

A recent section of this chapter deals with the existence of primitive roots for primes. In the present section, our main aim is to find the existence of primitive roots for composite numbers. We discourse this fact by square of a prime number, which are speculated in the following theorems.

Lemma 8.6.1. *If p is an odd prime having a primitive root r modulo p, then $r^{p-1} \not\equiv 1(\mathrm{mod}\ p^2)$.*

Proof. Since r is a primitive root modulo p, then the order of r is $\phi(p) = p - 1$. Also we have, $r^{p-1} \equiv 1(\mathrm{mod}\ p)$. Let n be the order of r modulo p^2, then $r^n \equiv 1(\ \mathrm{mod}\ p^2)$. This shows that $p^2\big|(r^n - 1) \Rightarrow p\big|r^n - 1$. Therefore $r^n \equiv 1(\mathrm{mod}\ p)$. Again Theorem 8.2.3 gives, $\phi(p) = (p-1)\big|n$ and Corollary 8.2.1 generates $n\big|\phi(p^2) = p(p-1)$. Now combining them, we can say that either $n = p - 1$ or $n = p(p-1)$. Finally, our task is to show $n = p - 1$ is not possible. Let us choose $s = r + p$ where s becomes a primitive root modulo p [$\because s \equiv r(\mathrm{mod}\ p)$]. Now applying Binomial Theorem,

$$\begin{aligned} s^{p-1} &= (r+p)^{p-1}, \\ &= r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \cdots + p^{p-1}, \\ &\equiv r^{p-1} + (p-1)r^{p-2}p(\ \mathrm{mod}\ p^2), \\ &\equiv r^{p-1} - pr^{p-2}(\ \mathrm{mod}\ p^2). \end{aligned}$$

From this congruence equation, we can assert that $s^{p-1} \not\equiv 1(\mathrm{mod}\ p^2)$. Otherwise, if $s^{p-1} \equiv 1(\mathrm{mod}\ p^2)$ holds then $pr^{p-2} \equiv 0(\mathrm{mod}\ p^2) \Rightarrow p^2|r^{p-2}p$. Thus $p|r^{p-2}$ ($\because \gcd(p, r) = 1$), which is not possible(Why!). This shows that for any primitive root r modulo p, $r^{p-1} \not\equiv 1(\mathrm{mod}\ p^2)$. □

In the preceding lemma, we have not considered the case $n = p(p-1)$. The following theorem shines on this case.

Theorem 8.6.1. *If p is an odd prime with primitive root r modulo p then either r or $r+p$ is a primitive root modulo p^2.*

Proof. Let n be the order of r modulo p^2. Then Lemma 8.6.1 yields, either $n = p-1$ or $n = p(p-1)$. Consider $n = p(p-1) = \phi(p^2)$. Then r becomes primitive root modulo p^2. Now, if $s = r+p$ then s becomes primitive root modulo p. Again, from the last Lemma we have $r^{p-1} \not\equiv 1(\bmod\, p^2)$. Hence the order of s modulo p^2 is $p(p-1) = \phi(p^2)$. Consequently $s = r+p$ is a primitive root modulo p^2. □

To illustrate the above theorem, let us pick-out $p = 11$. Then we get $2^{10} \equiv 1($ mod 11). This asserts, 2 is a primitive root modulo 11. Now, $2^{11(11-1)} = 2^{110} \equiv 1($ mod 121)(Verify!). Concluding that 2 is the primitive root of 121. Now if we choose, $p = 487$ then 10 will be the primitive root modulo 487. Here we can see that $497 = 487 + 10$ becomes the primitive root modulo 487^2. In fact, $p = 487$ is the smallest prime for which there exists a primitive root that is not also a primitive root modulo 487^2. Till now, our discussions are based on primitive root modulo p^2 for an arbitrary odd prime p. Now a fairly natural question presents itself: what will happen, if we take any integral exponents of p greater than 2. As a prelude, we need a technical lemma.

Lemma 8.6.2. *Let p be an odd prime and r be the primitive root of p such that $r^{p-1} \not\equiv 1(\bmod\, p^2)$. Then for each positive integer $n \geq 2$, we also have $r^{p^{n-2}(p-1)} \not\equiv 1(\bmod\, p^n)$.*

Proof. Let us apply the principle of mathematical induction on $n \geq 2$. From Theorem 8.6.1, we know that if p has a primitive root r then r is also primitive root modulo p^2 satisfying $r^{p-1} \not\equiv 1(\bmod\, p^2)$. So the lemma holds true for $n = 2$.

Let us assume that the lemma is true for all $n \geq 2$. This shows that $r^{p^{n-2}(p-1)} \not\equiv 1(\bmod\, p^n)$. Now we are to show the lemma is true for $n+1$. As p being an odd prime yields $\gcd(r, p) = \gcd(r, p^{n-1}) = \gcd(r, p^n) = 1$. Using Euler's theorem, we obtain

$$r^{p^{n-2}(p-1)} = r^{\phi(p^{n-1})} \equiv 1(\bmod\, p^{n-1}).$$

This shows that for any integer k, we have

$$r^{p^{n-2}(p-1)} = (1 + kp^{n-1}). \tag{8.6.1}$$

Here $p \nmid k$, otherwise $k = tp$ [for some integer t], contradicts our hypothesis $r^{p^{n-2}(p-1)} \not\equiv 1(\text{mod } p^n)$. Now taking p-th power on both sides of (8.6.1), we find

$$\begin{aligned} r^{p^{n-1}(p-1)} &= (1+kp^{n-1})^p \\ &= 1 + p(kp^{n-1}) + \binom{p}{2}(kp^{n-1})^2 + \cdots + (kp^{n-1})^p \\ &\equiv 1 + kp^n(\text{ mod } p^{n+1}) \end{aligned}$$

Since $p \nmid k$, then we get

$$r^{p^{n-1}(p-1)} \not\equiv 1(\text{ mod } p^{n+1}).$$

This establishes the validity of the incongruence for $n+1$. So by principle of mathematical induction the incongruence of the statement holds true for every $n \geq 2$. □

Thus, the last lemma allows us to state and prove the following theorem.

Theorem 8.6.2. *Let p be an odd prime and r be a primitive root modulo p^2. Then, for all positive integers n, r is a primitive root modulo p^n.*

Proof. Here, for any odd prime p, r is a primitive root modulo p^2. Then, for any $n > 2$, Lemma 8.6.2 indicates $r^{p^{n-2}(p-1)} \not\equiv 1(\text{mod } p^n)$. Let d be the order of r modulo p^n. Using, Corollary 8.2.1 we have $d|\phi(p^n) = p^{n-1}(p-1)$. Again, we see that $r^d \equiv 1(\text{mod } p^n) \Rightarrow r^d \equiv 1(\text{mod } p)$(How!). Also from Theorem 8.2.1 we have, $p-1 = \phi(p)\big|d$. Considering $d|p^{n-1}(p-1)$ and $(p-1)|d$ simultaneously, we obtain $d = p^t(p-1)$, where t is an integer such that $0 \leq t \leq n-1$. If we take $t < n-1$, then

$$r^{p^{n-2}(p-1)} = (r^{p^t(p-1)})^{p^{n-2-t}} \equiv 1(\text{ mod } p^n),$$

as d being the order of r modulo p^n. This contradicts the fact $r^{p^{n-2}(p-1)} \not\equiv 1(\text{mod } p^n)$. Hence $d = p^{n-1}(p-1) = \phi(p^n)$, consequently r becomes a primitive root modulo p^n. □

The following example will lucidly explain the foregoing theorem.

Example 8.6.1. Let us choose $p = 5$ then $\phi(5) = 4$. Now we show that $3^4 \equiv 1(\text{mod } 5)$. Here $3^{20} = (3^4)^5 \equiv 1(\text{mod } 25)$. Thus 3 is a primitive root modulo 5 and also for modulo 25. Then using Theorem 8.6.2 we can say that 3 is also a primitive root modulo 5^n, for all positive integers n. In fact, here we have shown it for $n = 3$. For that $\phi(p^3) = p^2(p-1) = 25 \times 4 = 100$. Now $3^5 \equiv (-7)(\text{mod } 125) \Rightarrow 3^{100} \equiv 7^{20} \equiv 1(\text{mod } 125)$, as $7^{10} \equiv (-1)(\text{mod } 125)$.

Till now, our discussion was based on primitive root modulo exponents of odd primes. Proceeding further, on primitive roots modulo powers of 2, we figure out 1 and 3 to be primitive roots modulo 2 and 2^2 respectively. Now, the following theorem furnishes a means for the situation modulo 2^n for $n > 2$. So let us begin with a technical lemma.

Lemma 8.6.3. *If a be an odd integer then* $a^{\frac{\phi(2^n)}{2}} = a^{2^{n-2}} \equiv 1(\bmod 2^n)$ *for any integer* $n \geq 3$.

Proof. Considering principle of mathematical induction on n, let $n = 3$. Then $a^2 \equiv 1(\bmod 8)$. Since a is an odd integer, let us take $a = 2m + 1$ where $m \geq 0$.

$$\therefore\ (2m+1)^2 \equiv 1(\bmod 8) \Rightarrow 4(m+1)m \equiv 0(\bmod 8).$$

Obviously $8\big|4m(m+1)$ as m being a non-negative integer and $m(m+1)$ is a product of consecutive integers. So the lemma is true for $n = 3$.

Let us assume the lemma is true for some integer $k > 3$. Then for any odd integer a the equivalence relation $a^{2^{k-2}} \equiv 1(\bmod 2^k)$ holds, which implies $\exists$ an integer d such that $a^{2^{k-2}} = 1 + d \cdot 2^k$. Squaring both sides, we obtain

$$\begin{aligned} a^{2^{k-1}} &= (1 + d2^k)^2, \\ &= 1 + d2^{k+1} + d^2 2^{2k}, \\ &\equiv 1(\bmod 2^{k+1}). \end{aligned}$$

This asserts that the lemma is true for $n = k + 1$. So the equivalence relation $a^{2^{n-2}} \equiv 1(\bmod 2^n)$ is true for all $n \geq 3$. ☐

Consequence of the last lemma leads to the next theorem.

Theorem 8.6.3. *The integer* 2^n *has no primitive root for* $n \geq 3$.

Proof. From the definition of primitive roots, it follows that if 2^n possesses a primitive root then it satisfies $a^{\phi(2^n)} \equiv 1(\bmod 2^n)$ for any odd integer a and $n \geq 3$. But Lemma 8.6.3 establish,

$$a^{2^{n-2}} = a^{\frac{\phi(2^n)}{2}} \equiv 1(\bmod 2^n).$$

So there are no primitive roots for $n \geq 3$. ☐

For further clarification, let us pick out $n = 4$ and $a = 5$. Then $\phi(2^4) = 8$. Here $5^{\frac{\phi(2^4)}{2}} = 5^4 \equiv 1(\bmod 2^4)$. So 5 is not a primitive root modulo 2^4. Now, instead of taking exponents of 2 or exponents of odd prime if we take a composite number which can be factored into a product of two relatively primes, then $\nexists$ any primitive roots modulo that composite number. Next theorem is based on that intent.

Theorem 8.6.4. *If for any two integers $m, n > 2$, $\gcd(m, n) = 1$ then the integer mn has no primitive root.*

Proof. Let us start with an integer a such that $\gcd(a, mn) = 1$. Then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Choose $b = lcm(\phi(m), \phi(n))$ and $d = \gcd(\phi(m), \phi(n))$. Theorem 7.2.4 guarantees that both $\phi(m)$ and $\phi(n)$ are even numbers, which implies $d \geq 2$. Also, Theorem 2.5.1 yields

$$b = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}. \; [\because \phi \text{ is multiplicative}]$$

From Euler's theorem we have, $a^{\phi(m)} \equiv 1(\bmod m)$ and $a^{\phi((n)} \equiv 1(\bmod n)$. Therefore $a^b = (a^{\phi(m)})^{\frac{\phi(n)}{d}} \equiv 1(\bmod m)$ and $a^b = (a^{\phi(n)})^{\frac{\phi(m)}{d}} \equiv 1(\bmod n)$. Since $\gcd(m, n) = 1$, combining we get $a^b \equiv 1(\bmod mn)$. But here $b \neq \phi(mn)$ which shows a is not a primitive root modulo mn. □

For further illustration of this theorem, choose $m = 3, n = 4$ and $a = 5$. Then $\phi(3 \times 4) = \phi(3) \times \phi(4) = 2 \times 2 = 4$. Now $5^2 = 25 \equiv 1(\bmod 12)$ shows 5 is not a primitive root modulo 12. We have demonstrated that all exponents of odd primes possess primitive roots. Also, the only powers of 2 which have primitive roots are 2 and 4. Consider the form $m = 2p^n$ where p is an odd prime and n is a positive integer. The following theorem deals with those forms of integers having primitive roots.

Theorem 8.6.5. *Let p be an odd prime and $n \geq 1$, then the form $2p^n$ possesses primitive roots.*

Proof. Let a be a primitive root modulo p^n. Then $a^{\phi(p^n)} \equiv 1(\bmod p^n)$. As ϕ is multiplicative so, $\phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$. Thus we have $a^{\phi(2p^n)} \equiv 1(\bmod p^n)$. Two cases may arise:

Case I a is odd: Then $a^{\phi(2p^n)} \equiv 1(\bmod 2)$. Now $\gcd(2, p) = 1 \Rightarrow \gcd(2, p^n) = 1 \Rightarrow a^{\phi(2p^n)} \equiv 1(\bmod 2p^n)$. This proves, a is a primitive root modulo $2p^n$.

Case II a is even: Then $a+p^n$ is odd. So $(a+p^n)^{\phi(2p^n)} \equiv 1(\bmod 2)$. As $a+p^n \equiv a(\bmod p^n)$, so $(a + p^n)^{\phi(2p^n)} \equiv 1(\bmod p^n)$. Therefore $(a + p^n)^{\phi(2p^n)} \equiv 1(\bmod 2p^n)$, by a similar argument as above. This shows $a+p^n$ is a primitive root modulo $2p^n$.

□

Referring to Example 8.6.1, 3 is a primitive root modulo $5^n (n \geq 1)$. Then from the above theorem, 3 also becomes a primitive root modulo $2 \cdot 5^n$. In fact, if we choose $n = 3$ then $m = 2 \times 5^3 = 250$ and $\phi(2 \times 5^3) = 5^2 \times 4 = 100$ holds. Here

$3^{20} = (3^5)^4 \equiv (-7)^4 \equiv 151 (\text{mod } 250)$. Finally, $3^{100} \equiv (151)^4 \equiv 1 (\text{mod } 250)$. This proves, 3 is a primitive root of 2×5^3. Again, if $a = 2$ then $2 + 5^n$ is odd for $n \geq 1$. From preceding theorem, $2 + 5^n$ becomes a primitive root modulo 2×5^n. In particular, if we prefer $n = 2$ then $2 + 5^2 = 27$ becomes a primitive root modulo $2 \times 5^2 = 50$, as $27^{20} = (27^5)^4 \equiv 7^4 \equiv 1 (\text{mod } 50)$.

Remark 8.6.1. *After discussing all the theorems and results in this section we are in this point to say that an integer $k > 1$ possesses a primitive root if and only if $k = 2, 4, p^n, 2p^n$, where p is an prime.*

8.7 Worked out Exercises

Problem 8.7.1. *Determine all the primitive roots of* $3^2, 3^3, \ \& \ 3^4$.

Solution 8.7.1. *Remark (8.6.1) guarantees the existence of primitive roots for* 3^k. *Here,* 2 *is a primitive root of* 3. *Therefore either* 2 *or* $2+3$ *will be primitive roots of* $3^k (k \geq 2)$. *If* r *be a primitive root of* p *then, order of* $r (\text{mod } p^2)$ *is* $p - 1$ *or* $p(p-1)$. *Hence order of* $2 (\text{mod } 3^2)$ *is* $3 - 1$ *or* $\phi(3^2)$. *But* $2^2 = 4 \equiv 1($ mod $3^2)$, *so* $2^{\phi(3^2)} \equiv 1 (\text{mod } 3^2)$. *Thus,* 2 *is a primitive root of* $3^2, 3^3, \ \& \ 3^4$. *Next, let us calculate the other primitive roots of* $3^2, 3^3, \ \& \ 3^4$.

(a) 3^2*: There are* $\phi(\phi(3^2)) = \phi(6) = 2$ *primitive roots. Since* $\phi(3^2) = 6$ *therefore,* 2^h *will have order* 6*(Why!)* $\iff$ $\gcd(h, 6) = 1$ *or* $h = 1, 5$. *Thus,*

$$2^5 = 32 \equiv 5(\text{ mod } 3^2).$$

Hence the primitive roots of 3^2 *are* $2, 5$.

(b) 3^3*: There are* $\phi(\phi(3^3)) = \phi(18) = 6$ *primitive roots and all are of the form* 2^k *such that* $\gcd(k, 18) = 1$ *or* $k = 1, 5, 7, 11, 13, 17$. *Thus,*

$$\begin{aligned}
2^5 &= 32 \equiv 5(\text{ mod } 27), \\
2^7 &\equiv 5 \cdot 2^2 \equiv 20(\text{ mod } 27), \\
2^{11} &\equiv 5^2 \cdot 2 = 50 \equiv 23(\text{ mod } 27), \\
2^{13} &\equiv 23 \cdot 2^2 = 92 \equiv 11(\text{ mod } 27), \\
2^{17} &\equiv 2^{11} \cdot 2^5 \cdot 2^2 \equiv 23 \cdot 5 \cdot 2 = 230 \equiv -40 \equiv 14(\text{ mod } 27).
\end{aligned}$$

Hence the primitive roots of 3^3 *are* $2, 5, 11, 14, 20, 23$

(c) 3^4*: Left to the reader.*

Problem 8.7.2. *Find the primitive root for all positive integers k modulo* 13^k.

Solution 8.7.2. *As* $2^{12} = 4096 \equiv 1(\bmod 13)$*, so* 2 *is a primitive root of* 13*. Here Theorem 8.6.1 can be brought into work to assert that either* 2 *or* $2+13 = 15$ *is a primitive root of* 13^2*. Now we have,* $2^{12} \equiv 40(\bmod 13^2)$ *and* $(2^{12})^{13} = 2^{156} \equiv 40^{13} \equiv 1(\bmod 13^2)$*. Therefore* 2 *is a primitive root of* 13^2*. So Theorem 8.6.2 asserts that* 2 *is a primitive root of* 13^k*.*

Problem 8.7.3. *Obtain a primitive root of* 34*.*

Solution 8.7.3. *Here we note that* $3^4 \equiv -4(\bmod 17) \Rightarrow 3^{16} \equiv 1(\bmod 17)$*. Hence* 3 *is a primitive root of* 17*. Appealing Theorem 8.6.5 we can conclude that* 3 *is a primitive root of* $2 \times 17 = 34$*.*

Problem 8.7.4. *For any odd prime* p*, prove that any primitive rootr of* p^n *is also a primitive root of* p*.*

Solution 8.7.4. *Here,*

$$\gcd(r, p^n) = 1 \Rightarrow \gcd(r, p) = 1.$$

Let k *be the order of* $r(\bmod p)$*.*

$$\begin{aligned} \therefore\ r^k &\equiv 1(\bmod p). \\ \therefore\ k \Rightarrow |\phi(p) &\Rightarrow k\big|(p-1). \end{aligned} \tag{8.7.1}$$

Also, $r^k = 1 + sp,\ s \in \mathbb{Z}$*. So for* $n > 1$ *we obtain*

$$\begin{aligned} r^{kp^{(n-1)}} &= (1+sp)^{p^{(n-1)}}, \\ &= 1 + \binom{p^{n-1}}{1} sp + \binom{p^{n-1}}{2} (sp)^2 + \ldots + (sp)^{p^{n-1}}. \\ \text{But, } p^{n-1}\Big| &\binom{p^{n-1}}{k}, \text{ for } 1 \le k \le p^{n-1}\ \& \\ p\big|(sp)^k&, \text{ for } 1 \le k \le p^{n-1}. \\ \therefore\ p^n\Big| &\left[\binom{p^{n-1}}{1} sp + \binom{p^{n-1}}{2} (sp)^2 + \ldots + (sp)^{p^{n-1}}\right]. \\ \therefore\ r^{kp^{n-1}} &\equiv 1(\bmod p^n). \end{aligned}$$

Since r *is a primitive root of* p^n*, therefore*

$$\begin{aligned} \phi(p^n)\big|kp^{n-1}&\ \text{[Why!]}, \\ \phi(p^n) &= p^{n-1}(p-1). \\ \therefore\ (p-1)\big|k&. \end{aligned} \tag{8.7.2}$$

Hence combining (8.7.1) and (8.7.2) yields $k = p - 1$*, so order of* $r \bmod p$ *is* $p - 1$*.*

Problem 8.7.5. *Prove that* 3 *is a primitive root of all integers of the form* 7^k *and* $2\cdot 7^k$.

Solution 8.7.5. *Here*

$$\begin{gathered}3^1 \not\equiv 1(\bmod 7),\ 3^2 \not\equiv 2(\bmod 7),\ 3^3 \not\equiv 6(\bmod 7),\\ 3^4 \not\equiv 4(\bmod 7),\ 3^5 \not\equiv 5(\bmod 7),\ 3^6 \equiv 1(\bmod 7).\end{gathered}$$

$$\therefore\ 3^{\phi(7)} = 3^6 \equiv 1(\bmod 7).$$

So 3 *is a primitive root of* 7. *Therefore order of* $3 \bmod 7^2$ *is* $7-1$ *or* $7(7-1)$.

$$\begin{aligned}\textit{But, } 3^4 &= 81 \equiv 32(\bmod 7^2).\\ \therefore\ 3^6 &\equiv 9\cdot 32 \equiv 43(\bmod 7^2).\\ \therefore\ 3^6 &\not\equiv 1(\bmod 7^2).\end{aligned}$$

Thus, order of $3(\bmod 7^2)$ *is* $\phi(7^2) = 7(7-1)$. *Now, Lemma 8.6.2 displays that for* $k \geq 2$,

$$3^{7^{(k-2)}(7-1)} \not\equiv 1(\bmod 7^k).$$

And Theorem 8.6.2 asserts 3 *is a primitive root of* 7^k, $k \geq 1$. *Finally,* 3 *being an odd primitive root for* 7^k, *Theorem 8.6.5 establishes that* 3 *is a primitive root of* $2\cdot 7^k$.

Problem 8.7.6. *Assume that* r *is a primitive root of the odd prime* p *and* $(r+tp)^{p-1} \not\equiv 1(\bmod p^2)$. *Show that* $r+tp$ *is a primitive root of* p^k *for each* $k \geq 1$.

Solution 8.7.6. *Since* $r \equiv (r+tp)(\bmod p)$, *so* r *and* $r+tp$ *have same order. Therefore* $r+tp$ *is also a primitive root of* p. *Since any primitive root of has order* $\bmod p^2$ *of* $p-1$ *or* $p(p-1)$, *then* $r+tp$ *has order modulo* p^2 *of* $p-1$ *or* $p(p-1)$. *By the given condition,* $(r+tp)^{p-1} \not\equiv 1(\bmod p^2)$, *order of* $r+tp$ *is not* $p-1$ *so must be* $\phi(p^2) = p(p-1)$. *Therefore* $r+tp$ *is a primitive root of* p, *is also a primitive root of* p^2. *Finally,* $r+tp$ *is a primitive root of* p^k *for each* $k \geq 1$ *[refer to Lemma 8.6.2 and Theorem 8.6.2].*

Problem 8.7.7. *Obtain all the primitive roots of* 41.

Solution 8.7.7. *With reference to Table 8.1 we see that* 6 *is a primitive root of* 41. *Also by Theorem 8.2.4 we can say that all other primitive roots are congruent to one of* $6, 6^2, \ldots, 6^{40}$. *Again,* 41 *has* $\phi(\phi(41)) = \phi(40) = (2^3-2^2)\times(5-1) = 16$ *incongruent primitive roots.*

Now by Theorem 8.2.3 we can assert, if 6 *has order* 40 *then* 6^b *has order* $\dfrac{40}{\gcd(b,40)}$. *Here* 6^b *will be a primitive root if* $\gcd(b,40) = 1$. *This implies,*

$$b = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.$$

Finally taking the above b's as exponent of 6*, we can find other primitive roots modulo* 41*(Do it!).*

Problem 8.7.8. *A Carmichael function, after the famous American Mathematician Robert Carmichael, associates to every positive integer* k *there exists a positive integer* v *such that* $\{a^v \equiv 1(\bmod k)\}$*, for all integers* a *with* $\gcd(a, k) = 1$*. Moreover, the least universal exponent of* k *is known to be the minimal universal exponent of* k*, denoted by* $\lambda(k)$*. Minimal universal exponent of* k *is often termed as reduced totient function or the least universal exponent. In general, if* $k = 2^m p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}$ *be the prime factorization of* $n(> 1)$ *then* $\lambda(k) = lcm(\lambda(2^m), \phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_r^{t_r}))$ *where* $\lambda(2) = 1,\ \lambda(2^2) = 2$ *and* $\lambda(2^m) = 2^{m-2}$ *for* $m \geq 3$*. Using the definition, prove the following statements:*

1. *For* $k = 2,\ 4,\ p^t,\ 2p^t$*, where* p *is an odd prime,* $\lambda(k) = \phi(k)$*.*
2. *If* $\gcd(a, 2^k) = 1$*, then* $a^{\lambda(2^k)} \equiv 1(\bmod 2^k)$*.*
3. *If* $\gcd(a, k) = 1$ *then* $a^{\lambda(k)} \equiv 1(\bmod k)$*.*

Solution 8.7.8.

1. *Pertaining the above definition, we find* $\lambda(2) = 1$*. Now* $\phi(2) = 2 - 2^0 = 1 \Rightarrow \lambda(2) = \phi(2)$*. Again, by virtue of the definition,* $\lambda(2^2) = 2 = 2^2 - 2^1 = \phi(2^2)$*. Now for* $k = 2p^t$*, we see that*

$$\lambda(k) = lcm(\lambda(2), \phi(p^t)) = lcm(1, \phi(p^t)) = \phi(p^t)\ \&$$
$$\phi(2\phi(p^t)) = \phi(2)\phi(\phi(p^t)) = \phi(\phi(p^t)).$$

   These two together gives $\lambda(2\phi(p^t)) = \phi(2\phi(p^t))$*. Similarly, for* $k = p^t$ *we get* $\lambda(\phi(p^t)) = \phi(\phi(p^t))$*.*

2. *Since* $\gcd(a, 2^k) = 1$ *then, by Euler's theorem we can say that* $a^{\phi(2^k)} \equiv 1(\bmod 2^k)$*. Taking mathematical induction into consideration, the problem prevails for* $k = 1, 2$ *[Verify!]. Consider the problem to be true for* $k = m \geq 3$*. Then we can assert that* $a^{\lambda(2^m)} \equiv 1(\bmod 2^m)$*. This shows that*

$$\begin{aligned} a^{\lambda(2^m)} &= 1 + 2^m r \\ \Rightarrow a^{2\lambda(2^m)} &= (1 + 2^m r)^2 \\ \Rightarrow a^{\lambda(2^{m+1})} &= 1 + 2 \cdot 2^m r + 2^{2m} r^2 \\ \Rightarrow a^{\lambda(2^{m+1})} &= 1 + 2^{m+1} r + 2^{m-1} 2^{m+1} r^2 \\ \Rightarrow a^{\lambda(2^{m+1})} &= 1 + (r + r^2 2^{m-1}) 2^{m+1}. \end{aligned}$$

   This shows that $a^{\lambda(2^{m+1})} \equiv 1(\bmod 2^{m+1})$*. Thus we can say that the result is true for all* k*.*

3. Let $k = p^t$*, p being an odd prime. Then by* (1) *we have* $\lambda(k) = \phi(k)$*. Since* $\gcd(a, k) = 1$ *then, by Euler's theorem* $a^{\lambda(k)} = a^{\phi(k)} \equiv 1 (\text{mod } k)$*. If* $k = 2^m p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$ *then, by (2) we see that* $a^{\lambda(2^m)} \equiv 1 (\text{mod } 2^m)$*. Since* $\lambda(2^m) \big| lcm[\lambda(2^m), \phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_r^{t_r})]$ *it follows* $a^{\lambda(k)} \equiv 1 (\text{mod } 2^m)$*. Again by Euler's theorem we have,* $a^{\phi(p_i^{t_i})} \equiv 1 (\text{mod } p_i^{t_i})$ *which further asserts that* $a^{lcm[\lambda(2^m), \phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_r^{t_r})]} \equiv 1 (\text{mod } p_i^{t_i})$*. Combining* $\lambda(p_i^{t_i}) = \phi(p_i^{t_i})$ *[by (1)] and* $\lambda(p_i^{t_i}) \big| lcm[\lambda(2^m), \phi(p_1^{t_1}), \phi(p_2^{t_2}), \dots, \phi(p_r^{t_r})]$*, it follows* $a^{\lambda(k)} \equiv 1 (\text{mod } p_i^{t_i})$*. This is true for all* $i = 1, 2, \dots, r$*. Finally, applying corollary(4.2.2) we can conclude that* $a^{\lambda(k)} \equiv 1 (\text{mod } k)$*.*

Problem 8.7.9. *Prove that if* $\gcd(a, k) = 1$*, then the linear congruence* $ax \equiv b(\text{mod } k)$ *has the solution* $x \equiv ba^{\lambda(k)-1} (\text{mod } k)$*.*

Solution 8.7.9. *By virtue of the Problem 8.7.8(3), we get* $a^{\lambda(k)} \equiv 1 (\text{mod } k)$*. Then, multiplying both sides of the congruence by b we get*

$$ba^{\lambda(k)} \equiv b(\text{ mod } k)$$
$$b \cdot a \cdot a^{\lambda(k)-1} \equiv b(\text{ mod } k)$$
$$a\big(ba^{\lambda(k)-1}\big) \equiv b(\text{ mod } k).$$

This shows that $x \equiv ba^{\lambda(k)-1} (\text{mod } k)$ *is a solution of* $ax \equiv b(\text{mod } k)$*.*

8.8 Index Arithmetic

The present section deals with an important aspect of modular arithmetic, introduced by Gauss in his Disquistiones Arithmeticae. Theorem(8.2.4) highlights the idea that if a is a primitive root modulo m then the integers $a^1, a^2, \cdots, a^{\phi(m)}$ forms a reduced system of modulo m. For any arbitrary integer r relatively prime to m, $\exists$ unique x with $1 \le x \le \phi(m)$, satisfies $a^x \equiv r(\text{mod } m)$. This motivates us to give the following definition.

Definition 8.8.1. *Let m be a positive integer with primitive root a. If r be another integer relatively prime to m, then* $\exists$ *unique integer x, with* $x(1 \le x \le \phi(m))$*, such that* $a^x \equiv r(\text{mod } m)$ *holds is said to be index of r base a modulo m.*

Also, this index is denoted as $\text{ind}\,{}_a^r$. Thus we can write $a^{\text{ind}\,{}_a^r} \equiv r(\text{mod } m)$. In fact, if x is an index of r base a then $x = \text{ind}\,{}_a^r$, where we do not need to indicate modulo m which is already prime to a. Choose any integer ŕ, which is also congruent modulo r. Then $r \equiv \acute{r}(\text{mod } m)$ where ŕ is also relatively prime to m. Hence $a^{\text{ind}\,{}_a^r} \equiv r(\text{mod } m)$ and $a^{\text{ind}\,{}_a^{\acute{r}}} \equiv \acute{r}(\text{mod } m)$ together imply $a^{\text{ind}\,{}_a^r} \equiv a^{\text{ind}\,{}_a^{\acute{r}}}(\text{mod } m)$. Finally an appeal to Theorem 8.2.2 concludes that

$\text{ind}\,_a^{r} \equiv \text{ind}\,_a^{\acute{r}}(\bmod \phi(m))$. The upcoming example will help to understand the notion of index.

Example 8.8.1. Pick out $m = 5$. Then $\phi(5) = 4 \Rightarrow 2^4 \equiv 1(\bmod 5)$. This shows that 2 is primitive root modulo 5. Now,

$$2^4 \equiv 1(\bmod 5),\ 2^3 \equiv 3(\bmod 5),\ 2^2 \equiv 4(\bmod 5),\ 2^1 \equiv 2(\bmod 5)$$

and it follows that

$$\text{ind}\,_2^{1} = 4,\ \text{ind}\,_2^{2} = 1,\ \text{ind}\,_2^{3} = 3,\ \text{ind}\,_2^{4} = 2.$$

The following theorem depicts some properties of indices similar to logarithms of real numbers. Here the equality sign in logarithms is replaced with congruence relation modulo m. Sometimes indices are called discrete logarithms of integers.

Theorem 8.8.1. *If m has a primitive root a and ind$\,_a^{r}$ denotes the index of a relative to a then,*

1. *ind*$\,_a^{1} \equiv 0(\bmod \phi(m))$.
2. *ind*$\,_a^{r_1 r_2} \equiv$ *ind*$\,_a^{r_1} +$ *ind*$\,_a^{r_2}(\bmod \phi(m))$.
3. $k \cdot$ *ind*$\,_a^{r} =$ *ind*$\,_a^{r^k}(\bmod \phi(m))$, *for* $k > 0$.

Proof. 1. As a is a primitive root modulo m, from Euler's theorem we have

$$a^{\phi(m) \equiv 1(\bmod m)},$$

where $\phi(m)$ is the smallest power of a which is congruent modulo m.

$$\therefore\ \text{ind}\,_a^{1} \equiv 0(\bmod m).$$

2. From the definition of indices we have,

$$a^{\text{ind}\,_a^{r_1}} \equiv r_1(\bmod m),$$
$$\text{and } a^{\text{ind}\,_a^{r_2}} \equiv r_2(\bmod m).$$

Multiplying the last two congruence gives,

$$a^{\text{ind}\,_a^{r_1} + \text{ind}\,_a^{r_2}} \equiv r_1 r_2(\bmod m).$$

Again,

$$a^{\text{ind}\,_a^{r_1 r_2}} \equiv r_1 r_2(\bmod m).$$

Now, the property of congruence yields,

$$a^{\text{ind}\,_a^{r_1 r_2}} \equiv a^{\text{ind}\,_a^{r_1} + \text{ind}\,_a^{r_2}}(\bmod m).$$

Finally, by virtue of Theorem 8.2.2, we obtain the desired property.

3. Using definition of indices, we have

$$a^{\text{ind}_{a}^{r^k}} \equiv r^k(\mod m)$$
$$\text{and } a^{k\cdot\text{ind}_{a}^{r}} \equiv (a^{\text{ind}_{a}^{r}})^k \equiv r^k(\mod m).$$

Then from the property of congruences, we obtain

$$a^{k\cdot\text{ind}_{a}^{r}} \equiv a^{\text{ind}_{a}^{r^k}} (\mod m).$$

Finally, applying Theorem 8.2.2 we get

$$k \cdot \text{ind}_{a}^{r} = \text{ind}_{a}^{r^k} (\mod \phi(m)).$$

$\square$

For an illustration of the above properties, let us consider the following example.

Example 8.8.2. *Let us choose,* $m = 7$ *then* $\phi(7) = 6$ *and* $a = 5$. *Now,*

$$5^1 \equiv 5(\mod 7), \quad 5^2 \equiv 4(\mod 7), \quad 5^3 \equiv 6(\mod 7),$$
$$5^4 \equiv 2(\mod 7), \quad 5^5 \equiv 3(\mod 7), \quad 5^6 \equiv 1(\mod 7).$$

Here we note that

$$ind_{5}^{6} = 3, \quad ind_{5}^{3} = 5, \quad ind_{5}^{4} = 2, \quad ind_{5}^{5} = 1, \quad ind_{5}^{2} = 4.$$

Let $r_1 = 5$ *and* $r_2 = 4$ *with* $\gcd(5,4) = 1$ *and* $m = 7$. *Now,*

$$ind_{5}^{20} \equiv ind_{5}^{5} + ind_{5}^{4} \equiv 1 + 2 \equiv 3(\mod 6).$$

Again,

$$20 \equiv 6(\mod 7) \Rightarrow ind_{5}^{20} \equiv ind_{5}^{6}(\mod 6).$$
$$\therefore\ ind_{5}^{4\times5} \equiv ind_{5}^{4} + ind_{5}^{5}(\mod \phi(7)).$$

Take $k = 2$, *then*

$$ind_{5}^{3^2} \equiv 2ind_{5}^{3} \equiv 2 \times 5 \equiv 4(\mod 6).\ \textit{Here}\ 9 \equiv 2(\mod 7).$$
$$\therefore\ ind_{5}^{9} \equiv ind_{5}^{2}(\mod 6).$$
$$\therefore\ ind_{5}^{3^2} \equiv 2ind_{5}^{3}(\mod \phi(7)).$$

Actually, this concept of indices has important applications in solving binomial congruences of the type $x^k \equiv r(\mod m), k \geq 2$ *where* m *is a positive integer having primitive root and* $\gcd(r,m) = 1$. *The following example will reflect on solving an equation of this type.*

Example 8.8.3. *Solve the congruence* $3x^4 \equiv 5 (\mathrm{mod}\ 11)$ *using indices.*

As $m = 11$, *so* $\phi(11) = 10$. *Also,* $2^{10} \equiv 1 (\mathrm{mod}\ 11)$. *Thus* 2 *is the primitive root modulo* 11. *Now the table of indices as follows:*

a	1	2	3	4	5	6	7	8	9	10
ind_2^a	10	1	8	2	4	9	7	3	6	5

$$
\begin{aligned}
ind_2^{3x^4} &\equiv ind_2^5 \equiv 4 (\ \mathrm{mod}\ 10).\\
\textit{Also, } ind_2^{3x^4} &\equiv ind_2^3 + 4 ind_2^x (\ \mathrm{mod}\ 10),\\
&\equiv 8 + 4ind_2^x (\ \mathrm{mod}\ 10).\\
\therefore\ 8 + 4ind_2^x &\equiv 4 (\ \mathrm{mod}\ 10).\\
\therefore\ 4ind_2^x &\equiv -4 (\ \mathrm{mod}\ 10),\\
&\equiv 6 (\ \mathrm{mod}\ 10).
\end{aligned}
$$

Since $\gcd(2, 10) = 2$ *from Theorem(4.2.2), we obtain*

$$
\begin{aligned}
2ind_2^x &\equiv 3 (\ \mathrm{mod}\ 5).\\
\therefore\ ind_2^x &\equiv 4, 9 (\ \mathrm{mod}\ 5).\\
\textit{Thus we have, } x &\equiv 2^4, 2^9 (\ \mathrm{mod}\ 11).\\
\textit{So } x &\equiv 5, 6 (\ \mathrm{mod}\ 11) \ \textit{ are the solutions here.}
\end{aligned}
$$

Now in this particular example, the number of primitive roots are given by $\phi(\phi(11)) = 4$. *In this solution, we have taken* 2 *as a primitive root. The other primitive roots are* $8, 7, 10$. *Now consider any one of them say* 7, *then the above table may differ but the final solution remains unaltered. Let's justify this with an illustration:*

a	1	2	3	4	5	6	7	8	9	10
ind_7^a	10	3	4	6	2	7	1	9	8	5

$$
\begin{aligned}
ind_7^{3x^4} &\equiv ind_7^5 \equiv 2 (\ \mathrm{mod}\ 10).\\
\textit{Also, } ind_2^{3x^4} &\equiv ind_7^3 + 4 ind_7^x (\ \mathrm{mod}\ 10),\\
&\equiv 4 + 4ind_7^x (\ \mathrm{mod}\ 10).\\
\therefore\ 4 + 4ind_2^x &\equiv 2 (\ \mathrm{mod}\ 10).\\
\therefore\ 4ind_2^x &\equiv -2 (\ \mathrm{mod}\ 10),\\
&\equiv 8 (\ \mathrm{mod}\ 10).
\end{aligned}
$$

Since, $\gcd(4,10)=2$,

$$2ind_{7}^{x} \equiv 4(\mod 5).$$
$$\therefore\ ind_{7}^{x} \equiv 7,2(\mod 5).$$
$$\textit{Thus we have, } x \equiv 7^7, 7^{20}(\mod 11).$$
$$\textit{So } x \equiv 5,6(\mod 11) \ \textit{ are the solutions here.}$$

Next, our focus will be on the congruence of the form $x^k \equiv r(\text{mod } m), k \geq 2$ where m is a positive integer having primitive root and $\gcd(r,m)=1$. To discuss further, let us have the following definition:

Definition 8.8.2. *If m and k are positive integer with* $\gcd(r,m)=1$ *for any integer r, then we say that r is a kth power residue m provided the congruence $x^k \equiv r(\text{mod } m), k \geq 2$ has a solution.*

Now our next theorem deals with the case where m possesses a primitive root of this type of congruence equations which are solvable.

Theorem 8.8.2. *Let m be a positive integer having a primitive root and* $\gcd(r,m) = 1$*. Then the congruence $x^k \equiv r(\text{mod } m), k \geq 2$ has a solution if and only if $a^{\frac{\phi(m)}{d}} \equiv 1(\text{mod } m)$, where* $\gcd(k,\phi(m)) = d$*; if it has a solution then there are exactly d number of incongruent solutions modulo m.*

Proof. Let a be a primitive root modulo m. We know that $x^k \equiv r(\text{mod } m), k \geq 2$ holds if and only if $k \text{ ind}_{a}^{x} = t\phi(m) + \text{ind}_{a}^{r}$ for some integer t. Now, $k \text{ ind}_{a}^{x} - t\phi(m) = \text{ind}_{a}^{r}$ becomes a linear diophantine equation. From Theorem 2.7.1, we can say that this equation possess a solution if $d|\text{ind}_{a}^{r}$. Also, there are d number of incongruent solutions. As $d|\text{ind}_{a}^{r} \Rightarrow \text{ind}_{a}^{r} = dn$ for some integer n. Thus,

$$\frac{\phi(m)}{d}\text{ind}_{a}^{r} = \frac{\phi(m)}{d} \times (dn),$$
$$\Rightarrow \frac{\phi(m)}{d}\text{ind}_{a}^{r} \equiv 0(\mod \phi(m)).$$
$$\therefore\ r^{\frac{\phi(m)}{d}} \equiv 1(\mod m).$$

□

Remark 8.8.1. *In particular,taking m as prime say p with* $\gcd(r,p)=1$*, the congruence $x^k \equiv r(\text{mod } m), k \geq 2$ has a solution if and only if $a^{\frac{p-1}{d}} \equiv 1(\text{mod } m)$ where $d = \gcd(k, p-1)$.*

Finally to fine tune the above theorem, let us illustrate it by an example:

Example 8.8.4. *Let us consider a congruence equation by* $x^2 \equiv 4 (\bmod 5)$*, taking* $m = 5$*. Then*

$$d = \gcd(2, \phi(5)) = \gcd(2, 4) = 2.$$

Here

$$\frac{\phi(m)}{d} = \frac{4}{2} = 2 \ \& \ 4^{\frac{\phi(m)}{d}} = 4^2 \equiv 1(\bmod 5),$$

holds. So using the foregoing theorem, the given congruence equation is solvable.

8.9 Worked out Exercises

Problem 8.9.1. *The following is a table of indices for the prime* 17 *relative to the primitive root* 3*:*

a	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
ind_{3}^{a}	*16*	*14*	*1*	*12*	*5*	*15*	*11*	*10*	*2*	*3*	*7*	*13*	*4*	*9*	*6*	*8*

With the aid of this table, solve the following congruences:

1. $x^{12} \equiv 13 (\bmod 17)$.
2. $8x^5 \equiv 10 (\bmod 17)$.

Solution 8.9.1. 1. *Here,* $x^{12} \equiv 13 (\bmod 17), \ \gcd(13, 17) = 1.$

$$\therefore \ 12 ind_{3}^{x} \equiv ind_{3}^{13} (\bmod 16), \ ind_{3}^{13} = 4.$$
$$\therefore \ 12 ind_{3}^{x} \equiv ind_{3}^{13} \equiv 4 (\bmod 16), \ \gcd(12, 16) = 4.$$

Dividing by 4*, we get* $3 ind_{3}^{x} \equiv 1 (\bmod 4)$*. Hence* $ind_{3}^{x} = 3, 7, 11, 15$*. Thus,* $x = 6, 7, 10, 11$ *(refer to the table). Therefore* $x \equiv 6, 7, 10, 11 (\bmod 17)$*.*

2. *Here* $8x^5 \equiv 10 (\bmod 17), \ \gcd(10, 17) = 1.$

$$\therefore ind_{3}^{8} + 5 ind_{3}^{x} \equiv ind_{3}^{10} (\bmod 16).$$
$$\Rightarrow 10 + 5 ind_{3}^{x} \equiv 3 (\bmod 16).$$
$$\Rightarrow 5 ind_{3}^{x} \equiv -7 (\bmod 16).$$

Since $\gcd(5, 16) = 1$*, therefore one solution do exists. This implies,*

$$15 ind_{3}^{x} \equiv -21 (\bmod 16),$$
$$\Rightarrow \ - ind_{3}^{x} \equiv -21 (\bmod 16),$$
$$\Rightarrow ind_{3}^{x} \equiv 21 (\bmod 16) \equiv 5 (\bmod 16).$$

Thus from table, $x = 5$*. Hence* $x \equiv 5 (\bmod 17)$*.*

Problem 8.9.2. *Find the remainder when* $3^{24} \cdot 5^{13}$ *is divided by* 17.

Solution 8.9.2. *Here* $3^{24} \cdot 5^{13} \equiv x(\mathrm{mod}\ 17)$ & $\gcd(1,17) = 1$, *so just one solution exists.*

$$
\begin{aligned}
&\therefore 24 ind_{3}^{3} + 13 ind_{3}^{5} \equiv ind_{3}^{x}(\ \mathrm{mod}\ 16)\\
&\Rightarrow 24(1) + 13(5) \equiv ind_{3}^{x}(\ \mathrm{mod}\ 16)\ [\textit{by Problem 8.9.1}].\\
&\Rightarrow 89 \equiv 9 \equiv ind_{3}^{x}(\ \mathrm{mod}\ 16),\\
&\therefore x \equiv 14(\ \mathrm{mod}\ 17).
\end{aligned}
$$

Hence remainder is 14.

Problem 8.9.3. *Show that the congruence* $x^3 = 3(\mathrm{mod}\ 19)$ *has no solutions, whereas* $x^3 = 11(\mathrm{mod}\ 19)$ *has three incongruent solutions.*

Solution 8.9.3.

1. *Here* $x^3 = 3(\mathrm{mod}\ 19)$ & $\gcd(3,19) = 1$. *Since* $\gcd(3,\phi(19)) = \gcd(3,18) = 3$ *and* $3^{\frac{18}{3}} = 3^6 = 3^3 - 3^3 \equiv 8 \cdot 8 \equiv 7 \not\equiv 1(\mathrm{mod}\ 19)$, *therefore* $x^3 = 3(\mathrm{mod}\ 19)$ *has no solutions[refer to Theorem 8.8.2].*

2. *Here* $x^3 = 11(\mathrm{mod}\ 19)$ & $\gcd(11,19) = 1$. *Since* $\gcd(3,\phi(19)) = \gcd(3,18) = 3$ *and* $11^{\frac{18}{3}} = 11^6 \equiv (-8)^6 \equiv (64)^3 \equiv (7)^3 \equiv 49 \cdot 7 \equiv 11 \cdot 7 \equiv 1(\mathrm{mod}\ 19)$, *therefore there are three incongruent solutions[refer to Theorem 8.8.2].*

Problem 8.9.4. *If* r *is a primitive root of the odd prime* p, *prove that*

$$ind_{r}^{-1} = ind_{r}^{p-1} = \frac{1}{2}(p-1).$$

Solution 8.9.4.

1. *Since* $-1 \equiv (p-1)(\mathrm{mod}\ p)$, *therefore* $ind_{r}^{-1} = ind_{r}^{p-1}$.

2. *Let* $x = ind_{r}^{p-1}$. *Then* $r^x \equiv (p-1)(\mathrm{mod}\ p)$. *As* p *is odd,* $p-1$ *is even. So* $\frac{p-1}{2}$ *exists.*

$$
\begin{aligned}
&\therefore\ r^{p-1} \equiv 1 \equiv (p-1)^2(\ \mathrm{mod}\ p)\\
&\Rightarrow\ r^{p-1} \equiv (p-1)^2(\ \mathrm{mod}\ p)\\
&\Rightarrow\ r^{\frac{p-1}{2}} \equiv (p-1)(\ \mathrm{mod}\ p)\ \textit{or}\ r^{\frac{p-1}{2}} \equiv -(p-1)(\ \mathrm{mod}\ p).
\end{aligned}
$$

If $r^{\frac{p-1}{2}} \equiv -(p-1)(\mathrm{mod}\ p) \equiv 1(\mathrm{mod}\ p)$, *then* r *would not have order* $p-1$ *(Why!). Hence* $r^{\frac{p-1}{2}} \equiv -(p-1)(\mathrm{mod}\ p) \not\equiv 1(\mathrm{mod}\ p)$. *So* $r^{\frac{p-1}{2}} \equiv (p-1)(\ \mathrm{mod}\ p)$ *holds. Thus by definition,* $ind_{r}^{p-1} = \frac{1}{2}(p-1)$.

Problem 8.9.5. *For which values of* b *is the exponential congruence* $9^x \equiv b(\ \mathrm{mod}\ 13)$ *solvable?*

Solution 8.9.5. *Here* 2 *is a primitive root of* 13*(check!). To solve, we need to construct the following table:*

a	1	2	3	4	5	6	7	8	9	10	11	12
$ind\,{}_{2}^{a}$	12	1	4	2	9	5	11	3	8	10	7	6

Therefore $x\,ind\,{}_{2}^{9} \equiv ind\,{}_{2}^{b}(\mathrm{mod}\ 12)$*, because* $ind\,{}_{2}^{9} = 8$*. Since* $\gcd(8,12) = 4$*, therefore the foregoing congruence yields* $4\big|ind\,{}_{2}^{b}$*. This implies* $ind\,{}_{2}^{b} = 4, 8, 12$*. Thus, from the above table we find* $b = 3, 9, 1$*.*

Problem 8.9.6. *Determine the integers* $a(1 \leq a \leq p-1)$ *such that the congruence* $x^4 \equiv a(\mathrm{mod}\ p)$ *has a solution for* $p = 7, 11,$ *&* 13*.*

Solution 8.9.6. *Since* $3^6 \equiv 1(\mathrm{mod}\ 7)$ *and* $2^{10} \equiv 1(\mathrm{mod}\ 11)$ *therefore,* $3, 2$ *is the primitive root of* $7, 11$ *respectively. To construct the table of indices for* 7*, the following congruences will be particularly helpful:*

$$3^1 \equiv 3(\ \mathrm{mod}\ 7),\ 3^2 \equiv 2(\ \mathrm{mod}\ 7),\ 3^3 \equiv 6(\ \mathrm{mod}\ 7),$$
$$3^4 \equiv 4(\ \mathrm{mod}\ 7),\ 3^5 \equiv 5(\ \mathrm{mod}\ 7),\ 3^6 \equiv 1(\ \mathrm{mod}\ 7).$$

Thus the corresponding table is as follows:

a	1	2	3	4	5	6
$ind\,{}_{3}^{a}$	6	2	1	4	5	3

Again, the following congruences will provide assistance in constructing the table of indices for 11*:*

$$2^1 \equiv 2(\ \mathrm{mod}\ 11),\ 2^2 \equiv 4(\ \mathrm{mod}\ 11),\ 2^3 \equiv 8(\ \mathrm{mod}\ 11),$$
$$2^4 \equiv 5(\ \mathrm{mod}\ 11),\ 2^5 \equiv 10(\ \mathrm{mod}\ 11),\ 2^6 \equiv 9(\ \mathrm{mod}\ 11),$$
$$2^7 \equiv 7(\ \mathrm{mod}\ 11),\ 2^8 \equiv 3(\ \mathrm{mod}\ 11),\ 2^9 \equiv 6(\ \mathrm{mod}\ 11),\ 2^{10} \equiv 1(\ \mathrm{mod}\ 11).$$

So the required table is:

a	1	2	3	4	5	6	7	8	9	10
$ind\,{}_{2}^{11}$	10	1	8	2	4	9	7	3	6	5

1. $p = 7$*:*

$$x^4 \equiv a(\ \mathrm{mod}\ 7),$$
$$4ind\,{}_{x} \equiv ind\,{}_{a}(\ \mathrm{mod}\ 6),\ \gcd(4,6) = 2.$$
$$\therefore\ 2\big|a \Rightarrow ind\,{}_{a} = 2, 4, 6.$$

Hence $a = 2, 4, 1$

2. $p = 11$*: left to the reader.*

3. $p = 13$*: left to the reader.*

Problem 8.9.7. *If* r *and* r' *are both primitive roots of the odd prime* p*, show that for* $\gcd(a, p) = 1$

$$ind\,{}^{a}_{r'} \equiv ind\,{}^{a}_{r}\, ind\,{}^{r}_{r'} (\mod p-1).$$

Solution 8.9.7. *Let* $x \equiv ind\,{}^{a}_{r'}(\bmod p)$, $y \equiv ind\,{}^{a}_{r}(\bmod p)$ & $z \equiv ind\,{}^{r}_{r'}(\mod p)$.

$$\begin{aligned} \therefore \textit{ by definition } (r')^x &\equiv a(\mod p),\\ (r)^y &\equiv a(\mod p)\ \&\\ (r')^z &\equiv r(\mod p) \Rightarrow (r')^{zy} \equiv (r)^y(\mod p).\\ \therefore\ (r')^x &\equiv (r)^y(\mod p) \equiv (r')^{zy}(\mod p).\end{aligned}$$

By Theorem 8.2.2, $x \equiv zy(\bmod p{-}1)$*. Therefore* $ind\,{}^{a}_{r'} \equiv ind\,{}^{a}_{r}\, ind\,{}^{r}_{r'}(\bmod p{-}1)$*.*

8.10 Exercises:

1. Find the order of the integers 2, 3 and 5 modulo 23.

2. If a has order $2k$ modulo odd prime p, then show that $a^k \equiv -1(\bmod p)$.

3. Prove that $\phi(2^n - 1)$ is a multiple of n for any $n > 1$.

4. Verify: The odd prime divisors of the integer n^2+n+1 which are different from 3 are of the form $6k + 1$.

5. Find two primitive roots of 10.

6. Prove that for any odd prime p, the prime divisors of $2^p - 1$ are of the form $2kp + 1$.

7. If p be an odd prime then show that the congruence $x^{p-2}+\ldots+x^2+x+1 \equiv 0(\mod p)$ has exactly $p - 2$ incongruent solutions and they are the integers $2, 3, \ldots, p - 1$.

8. If 3 is a primitive root of 43 then prove that all the positive integers less than 43 has the order 21 modulo 43.

9. Find all positive integers less than 61 having order 4 modulo 61.

10. Let r be a primitive root of the odd prime p. Show that if $p \equiv 3(\bmod 4)$ holds then $-r$ has order $\frac{p-1}{2}$ modulo p.

11. Find all primitive roots of 82 and 38.

12. Prove that the integer 20 has no primitive roots.

13. Obtain a primitive root for any integer k of the form 11^k and 17^k.

14. For any odd prime p show that there are as many primitive roots of $2p^n$ as of p^n.

15. Solve the following congruences by using a table of indices for a primitive root of 11:

    (a) $7x^3 \equiv 3(\bmod 11)$.

    (b) $x^8 \equiv 10(\bmod 11)$.

16. Constructing a table of indices for the prime 17 with respect to the primitive root 5, solve $7^x \equiv 7(\bmod 17)$.

17. Determine the integers $a(1 \leq a \leq 12)$ such that the congruence $ax^4 \equiv b($ mod 13) has a solution for $b = 2, 5,$ and 6.

18. Determine whether the two congruences $x^5 \equiv 13(\bmod 23)$ and $x^7 \equiv 15($ mod 29) are solvable.

19. Find the solutions of the exponential congruences $5^x \equiv 4(\bmod 19)$ and $4^x \equiv 13(\bmod 17)$.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

9

Theory of Quadratic Residues

> *"Mathematicians are like Frenchmen: whatever you say to them they translate into their own language and forthwith it is something entirely different."*
>
> – Johann Wolfgang von Goethe

9.1 Introduction

In the chapter Fermat's little theorem, we defined quadratic congruence equation of the form $ax^2 + bx + c \equiv 0(\bmod p)$, p being an odd prime and $a \not\equiv 0(\bmod p)$. There we have discoursed the solution of the quadratic congruence of the type $x^2 + 1 \equiv (\bmod p)$. Also, how to solve a quadratic congruence of that form, was being treated there. Following the path of solving a quadratic congruence, we need an important fact of modern number theory, known as quadratic reciprocity law, a major contribution of Gauss in 1796. After that many eminent mathematicians of 19th century had given their important contributions on this aspect. In the present chapter we have illustrated various important facts and results based on quadratic reciprocity law.

9.2 Quadratic Residues and Nonresidues

As quadratic reciprocity law deals with solving a quadratic congruences of the type $ax^2 + bx + c \equiv 0(\bmod p)$, p being an odd prime with $\gcd(a, p) = 1$. Also,

$\gcd(a, p) = 1 \Rightarrow \gcd(4a, p) = 1$. Multiplying $4a$ to both sides of the congruence, we obtain

$$(2ax + b)^2 \equiv b^2 - 4ac(\mod p).$$

Taking $t = 2ax + b$ and $d = b^2 - 4ac$, we get

$$t^2 \equiv d(\mod p).$$

If $x \equiv x_0 (\mod p)$ is a solution of first congruence then $t \equiv 2ax_0 + b(\mod p)$ is the solution of second one.

Conversely, if $t \equiv t_0 (\mod p)$ is a solution of second congruence then $2ax \equiv (t_0 - b)(\mod p)$ refers to the solution of first one. This leads us to the fact that instead of finding the solution of $ax^2 + bx + c \equiv 0(\mod p)$, we can find the solution of $t^2 \equiv d(\mod p)$. Turning on, towards solving the congruence $t^2 \equiv d(\mod p)$ if $p|d$ then $t \equiv 0(\mod p)$ is the only solution. Without any loss of generality, if we assume $p \nmid d$ then finding the solution of the type $x^2 \equiv r(\mod p)$ with $\gcd(r, p) = 1$ we need to identify those integers r which are perfect squares modulo p. The integer r associated with the forgoing congruence is commonly known as quadratic residue of p.

Definition 9.2.1. *Let p be an odd prime and r be an integer with $\gcd(r, p) = 1$. Then r is called quadratic residue modulo p, provided the congruence $x^2 \equiv r(\mod p)$ has a solution. If the congruence $x^2 \equiv r(\mod p)$ has no solution, then r is called quadratic nonresidue modulo p.*

Remark 9.2.1. *For any two integers r and s, if $r \equiv s(\mod p)$ holds then s is also quadratic residue modulo p if r is so.*

Example 9.2.1. *Set $p = 7$. Taking square of the integers from the set $\{1, 2, 3, 4, 5, 6\}$, the quadratic residues of 7 are 1, 2 and 4 as $1^2 \equiv 6^2 \equiv 1(\mod 7)$, $3^2 \equiv 4^2 \equiv 1(\mod 7)$, $5^2 \equiv 4(\mod 7)$ and $2^2 \equiv 4(\mod 7)$. Here $3, 5,$ and 6 are quadratic nonresidues of 7.*

The last example highlights the fact that 7 is an odd prime and for that we get three quadratic residue $1, 2$ and 4; three quadratic nonresidues $3, 5$ and 6. In general, for any odd prime p, the number of quadratic residues and quadratic nonresidues are both $\frac{p-1}{2}$ taken from the set $\{1, 2, \cdots, p-1\}$. The above discussion furnishes a pleasant opportunity for the following theorem.

Theorem 9.2.1. *If p is an odd prime, then the number of quadratic residues modulo p are $\frac{p-1}{2}$.*

Proof. Here, the quadratic residue is of the form $x^2 \equiv r(\bmod p)$ where p is the odd prime and r be an integer with $\gcd(r, p) = 1$. To compute quadratic residue of p among the integers $1, 2, \cdots, p-1$, we first need to establish that the number of incongruent solutions modulo p be either zero or two. Set $x = b$ as a solution and $(-b)^2 = b^2 \equiv r(\bmod p)$. Then $x = -b$ is also a solution of $x^2 \equiv r(\bmod p)$. Here $b \not\equiv -b(\bmod p)$ otherwise $b \equiv -b(\bmod p)$ implies $2b \equiv 0(\bmod p)$, which is not possible as $b^2 \equiv r(\bmod p)$ and $p \nmid r$. There exist no other solutions of the given equation as $x^2 \equiv b^2(\bmod p)$ implies $p\big|(x-b)(x+b)$. Then either $p|(x-b) \Rightarrow x \equiv b(\bmod p)$ or $p|(x+b) \Rightarrow x \equiv -b(\bmod p)$. Because the number of incongruent solutions are two, there must be exactly $\dfrac{p-1}{2}$ quadratic residues and non quadratic residues modulo p taken from $1, 2, \cdots, p-1$. ☐

The last theorem enables us to determine the number of quadratic residues taken from $1, 2, \cdots, p-1$. Now we pose the following question: Under what circumstances an integer r becomes a quadratic residue of odd prime p? In order to answer this question, we need the Euler's Criterion.

Theorem 9.2.2. *(Euler's Criterion): Let p be an odd prime with* $\gcd(r, p) = 1$. *Then r is a quadratic residue modulo p if and only if* $r^{\frac{p-1}{2}} \equiv 1(\bmod p)$.

Proof. Let r be a quadratic residue modulo p. Then $\exists\, b \in \{1, 2, \cdots, p-1\}$ such that $b^2 \equiv r(\bmod p)$. This implies, $b^{p-1} \equiv r^{\frac{p-1}{2}}(\bmod p)$. Then with the use of Fermat's theorem, we have $r^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1(\bmod p)$ as $\gcd(b, p) = 1$.

Conversely if $r^{\frac{p-1}{2}} \equiv 1(\bmod p)$, then $r^{\frac{p-1}{2}} \equiv 1(\bmod p)$. Let b be a primitive root modulo p. Then $r \equiv b^i(\bmod p)$ for some integer i where $1 \le i \le p-1$. This shows, $b^{\frac{i(p-1)}{2}} \equiv r^{\frac{p-1}{2}} \equiv 1(\bmod p)$. By Theorem 8.2.1 the order of b must divide $\dfrac{i(p-1)}{2}$. As b is a primitive root, so its order is $\phi(p) = p-1$. Thus to divide $\dfrac{i(p-1)}{2}$, i must be even, say $2j$. It follows that, $(b^j)^2 = b^{2j} = b^i \equiv r(\bmod p)$. Hence b^j is a solution of $x^2 \equiv r(\bmod p)$. This proves that r is quadratic residue of p.

As p is odd prime and $\gcd(r, p) = 1$, an appeal to Fermat's little theorem yields, $(r^{\frac{p-1}{2}} - 1)(r^{\frac{p-1}{2}} + 1) \equiv r^{p-1} - 1 \equiv 0(\bmod p)$. Thus, either $r^{\frac{p-1}{2}} \equiv 1(\bmod p)$ or $r^{\frac{p-1}{2}} \equiv -1(\bmod p)$ holds. Here both the conditions fail to agree together, otherwise $1 \equiv -1(\bmod p)$ implies $p|2$ leads to a contradiction. As $r^{\frac{p-1}{2}} \equiv 1(\bmod p)$ prevails for quadratic residue modulo p, then obviously $r^{\frac{p-1}{2}} \equiv -1(\bmod p)$ holds for quadratic non residue modulo p. ☐

The last part of the theorem generates an obvious corollary.

Corollary 9.2.1. *Let* p *be an odd prime with* $\gcd(r,p)=1$*. Then* r *is a quadratic residue modulo* p *or quadratic non residue modulo* p *according as* $r^{\frac{p-1}{2}} \equiv 1(\bmod p)$ *or* $r^{\frac{p-1}{2}} \equiv -1(\bmod p)$ *prevails.*

The next example illustrates Euler's Criterion.

Example 9.2.2. *If* $p=11$*, we have* $3^{\frac{11-1}{2}} = 3^5 \equiv 1(\bmod 11)$*. Also* $4^{\frac{11-1}{2}} = 4^5 \equiv 1(\bmod 11)$*. So* 3 *and* 4 *are quadratic residue modulo* 11*.*

Unlike our earlier discussions, from now on our efforts will be simplified by the symbol $(\frac{r}{p})$. As the notation $(\frac{r}{p})$ was introduced by Legendre, it is called Legendre symbol.

Definition 9.2.2. *Let* p *be an odd prime and* r *be an integer with* $\gcd(r,p)=1$*, then the Legendre symbol* $(\frac{r}{p})$ *is defined as,*

$$\left(\frac{r}{p}\right) = \begin{cases} 1, & \textit{if } r, \textit{ is a quadratic residue modulo } p; \\ -1, & \textit{if } r, \textit{ is a quadratic non residue modulo } p \end{cases}$$

For example, if we take $p=7$, the Legendre symbol can be expressed as $\left(\frac{1}{7}\right)=\left(\frac{2}{7}\right)=\left(\frac{4}{7}\right)=1$ and $\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{6}{7}\right)=-1$ as $1,2,4$ are quadratic residue modulo 7 and $3,5,6$ are quadratic non residue modulo 7.

By virtue of Legendre symbol, Euler's criterion can be portrayed as

$$\left(\frac{r}{p}\right) \equiv r^{\frac{p-1}{2}} (\bmod p).$$

The following theorem discourse few properties related to Legendre symbol.

Theorem 9.2.3. *Let* p *be an odd prime and* r,s *be integers not divisible by* p*. Then*

1. *If* $r \equiv s(\bmod p)$ *then* $(\frac{r}{p}) = (\frac{s}{p})$*.*

2. $(\frac{r}{p})(\frac{s}{p}) = (\frac{rs}{p})$*.*

3. $(\frac{r^2}{p}) = 1$*.*

Proof. 1. As $r \equiv s(\bmod p)$ then $x^2 \equiv r(\bmod p)$ has a solution if and only if $x^2 \equiv s(\bmod p)$ has a solution. Hence with respect to modulo p we have $(\frac{r}{p}) = (\frac{s}{p})$.

2. If $p|rs$ then the proof is obvious. Consider the case when $p \nmid rs$ and here $\gcd(p, rs) = 1$. By virtue of Euler's Criterion,
$$\begin{aligned}(\frac{rs}{p}) &\equiv (rs)^{\frac{p-1}{2}} (\mod p)\\ (\frac{rs}{p}) &\equiv (r)^{\frac{p-1}{2}} (s)^{\frac{p-1}{2}} (\mod p)\\ (\frac{rs}{p}) &\equiv \left(\frac{r}{p}\right)\left(\frac{s}{p}\right) (\mod p).\end{aligned}$$
Here Legendre symbol assume the values 1 and -1. If possible, let $(\frac{rs}{p}) \neq (\frac{r}{p})(\frac{s}{p})$. Then $1 \equiv -1 (\mathrm{mod}\ p) \Rightarrow p|2$, which is impossible. Thus $(\frac{r}{p})(\frac{s}{p}) = (\frac{rs}{p})$.

3. As $(\frac{r}{p})$ is either 1 or -1, it follows $(\frac{r^2}{p}) \equiv (\frac{r}{p})(\frac{r}{p}) \equiv 1 (\mathrm{mod}\ p)$. Hence we are done.

□

We now consider the problem of finding Legendre symbol of those prime p whose quadratic residue is -1. This can be achieved by Euler's Criterion.

Theorem 9.2.4. *If p is an odd prime, then*
$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv 1 (\mod 4)\\ -1, & \textit{if } p \equiv 3 \equiv -1 (\mod 4)\end{cases}$$

Proof. For any integer k, if $p \equiv 1 (\mathrm{mod}\ 4)$ then p is of the form $p = 4k + 1$. By Euler's criterion we have,
$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 (\mod p).$$
Also, for some integer k', if $p \equiv 3 (\mathrm{mod}\ 4)$ then p is of the form $p = 4k' + 3$. By similar reasoning as above we get,
$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k'+1} \equiv -1 (\mod p).$$
This proves,
$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 (\mod 4)\\ -1, & \text{if } p \equiv 3 \equiv -1 (\mod 4).\end{cases}$$

□

The last theorem depicts that the congruence equation of the form $x^2 \equiv -1 (\mod p)$ has at least one solution if and only if p is of the form $p = 4k + 1$ for any integer k. Now we must dispose of an example supporting the fact.

Example 9.2.3. *Let us consider the congruence* $x^2 \equiv 50 (\bmod 17)$*. We have to examine the solvability of this equation. This can be accomplished by evaluating* $(\frac{50}{17})$*. Now* $50 \equiv -1 (\bmod 17)$ *yields* $(\frac{50}{17}) = (\frac{-1}{17})$*. But from Euler's Criterion it follows,* $(\frac{-1}{17}) \equiv (-1)^{\frac{17-1}{2}} \equiv 1 (\bmod 17)$*, which asserts* $(\frac{50}{17}) = (\frac{-1}{17}) = 1$*. This testify the solvability of* $x^2 \equiv 50 (\bmod 17)$*.*

The following theorem dispense an important application regarding the number of odd primes.

Theorem 9.2.5. *For any positive integer* k*, There are infinitely many primes of the form* $4k+1$*.*

Proof. In anticipation of a contradiction, assume that there are finitely many primes $p_1, p_2, \cdots p_m$ and consider $N = (2p_1p_2\cdots p_m)^2 + 1$. Here N is odd so there exists some odd prime p which divides N. Thus $(2p_1p_2\cdots p_m)^2 \equiv -1 (\bmod p)$. Now an appeal to Theorem 9.2.4 renders that the Legendre symbol $(\frac{-1}{p}) = 1$ prevails if and only if $p = 4k+1$ for some positive integer k. This confirms that p is one of $p_1, p_2, \cdots p_m$. Hence $p_i \big| [N - (2p_1p_2\cdots p_m)^2]$ or $p_i \big| 1$ for any $i = 1, 2, \cdots m$. This contradicts the fact that there are finitely many primes of the form $4k+1$. Hence the proof. $\square$

Theorem 9.2.6. *If* p *is an odd prime then* $\sum_{r=1}^{p-1} (\frac{r}{p}) = 0$*, where both the number of quadratic residue and non residue modulo* p *are exactly* $\frac{p-1}{2}$*.*

Proof. Let a be a primitive root of p. Then by Theorem 8.2.4 the integers $a^1, a^2, \cdots a^{p-1}$ forms a reduced residue system modulo p, where $\phi(p) = p-1$. Let r be any integer between 1 and $p-1$. Then for a unique positive integer $k (1 \leq k \leq p-1)$, $r \equiv a^k (\bmod p)$ holds. Now with the aid of Euler's Criterion, we find

$$\left(\frac{r}{p}\right) = \left(\frac{a^k}{p}\right) \equiv (a^k)^{\frac{p-1}{2}} \equiv (a^{\frac{p-1}{2}})^k \equiv (-1)^k (\bmod p).$$

As a is a primitive root of p and $\gcd(a,p) = 1$, then $a^{\frac{p-1}{2}} \equiv -1 (\bmod p)$. But both $(\frac{r}{p})$ and $(-1)^k$ are equal to either 1 or -1. Hence $\sum_{r=1}^{p-1} (\frac{r}{p}) = \sum_{k=1}^{p-1} (-1)^k = 0$. It follows both the number of quadratic and quadratic nonresidues are exactly $\frac{p-1}{2}$. $\square$

The proof of the last theorem generates an important fact, which we have in the form of following corollary.

Corollary 9.2.2. *Let* p *be an odd prime. Then the quadratic residues of* p *are congruent modulo* p *to the even powers of a primitive root* a *of* p*; the quadratic nonresidues are congruent to the odd powers of* a*.*

Proof. Follows from the fact $(\frac{r}{p}) = (\frac{a^k}{p}) \equiv (-1)^k (\text{mod } p)$ of the foregoing theorem. □

For an exemplification of the fact, set $p = 7$. Here 3 is a primitive root modulo 7. By the even powers of 3, the quadratic residues modulo 7 are given by $3^2 \equiv 2(\text{mod } 7)$, $3^4 \equiv 4(\text{mod } 7)$ and $3^6 \equiv 1(\text{mod } 7)$; by the odd powers of 3, the quadratic nonresidues modulo 7 are $3^1 \equiv 3(\text{mod } 7)$, $3^3 \equiv 6(\text{mod } 7)$ and $3^5 \equiv 5(\text{mod } 7)$.

We are in a position to state and prove an elegant result due to Gauss. The result provides another criterion to find out whether an integer a relatively prime to p is a quadratic residue modulo p.

Theorem 9.2.7. *(Gauss Lemma): Let p be an odd prime and r be an integer with* $\gcd(r, p) = 1$. *If i denotes the number of integers among* $r, 2r, \cdots (\frac{p-1}{2})r$ *where remainders exceed by* $\frac{p}{2}$ *when divided by p, then* $(\frac{r}{p}) = (-1)^i$.

Proof. Here none of the integers among $r, 2r, \cdots (\frac{p-1}{2})r$ are congruent to zero modulo p as $\gcd(r, p) = 1$. Let $r_1, r_2, \cdots r_j$ be the remainders, when divided by p and $0 < r_k < \frac{p}{2}(k = 1, 2, \cdots j)$. Also, $s_1, s_2, \cdots s_i$ are the remainders when divided by p and $p > s_t > \frac{p}{2}(t = 1, 2, \cdots i)$. Then $i + j = (\frac{p-1}{2})$ and the integers, $r_1, r_2, \cdots r_j, p - s_1, p - s_2, \cdots p - s_i$ are all positive and less than $\frac{p}{2}$.

Claim: $p - s_t \neq r_k$. If not, let us choose $p - s_t = r_k$ for some t and k. Then $\exists\ u, v \in \mathbb{Z}$ with $1 \leq u, v \leq \frac{p-1}{2}$ satisfying $s_t \equiv ur(\text{mod } p)$ and $r_k \equiv vr(\text{mod } p)$. Then, $(u + v)r \equiv s_t + r_k \equiv p \equiv 0(\text{mod } p)$. As $\gcd(r, p) = 1$ so $(u + v)r \equiv 0(\text{mod } p)$. But this is impossible as $1 < u + v \leq p - 1$. Now the integers $r_1, r_2, \cdots r_j, p - s_1, p - s_2, \cdots p - s_i$ are among $1, 2, \cdots \frac{p-1}{2}$ in some order. So their product gives,

$$\left(\frac{p-1}{2}\right)! = r_1 r_2 \cdots r_j (p - s_1(p - s_2) \cdots (p - s_i)$$
$$\left(\frac{p-1}{2}\right)! \equiv r_1 r_2 \cdots r_j (-s_1)(-s_2) \cdots (-s_i)(\text{ mod } p)$$
$$\left(\frac{p-1}{2}\right)! \equiv (-1)^i r_1 r_2 \cdots r_j s_1 s_2 \cdots s_i(\text{ mod } p).$$

Also, the integers $r_1, r_2, \cdots r_j, p - s_1, p - s_2, \cdots p - s_i$ are congruent modulo p among $r, 2r, \cdots (\frac{p-1}{2})r$ in some order. Hence

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^i r(2r) \cdots \left(\left(\frac{p-1}{2}\right)r\right)(\text{ mod } p)$$
$$\left(\frac{p-1}{2}\right)! \equiv (-1)^i r^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!(\text{ mod } p).$$

As $\gcd(p, (\frac{p-1}{2})!) = 1$ so $1 \equiv (-1)^i r^{\frac{p-1}{2}} (\bmod\ p)$. Now by Euler's Criterion, $(\frac{r}{p}) \equiv r^{\frac{p-1}{2}} \equiv (-1)^i (\bmod\ p)$. This implies that, $(\frac{r}{p}) = (-1)^i$. □

Example 9.2.4. *Let* $r = 4$ *and* $p = 7$. *To find* $(\frac{4}{7})$ *compute the positive residues of* $1 \cdot 4,\ 2 \cdot 4,\ 3 \cdot 4$. *They are* $4, 1, 5$ *modulo* 7 *respectively. Since exactly two of the integers are greater than* $\frac{7}{2}$, *then from Gauss Lemma we can say that* $(\frac{4}{7}) = (-1)^2 = 1$. *This shows that* 4 *is a quadratic residue modulo* 7.

Now in later part of the present section, by Gauss Lemma, we have characterized all primes p that have 2 as a quadratic residue modulo p.

Theorem 9.2.8. *If* p *is an odd prime, then* $\left(\frac{2}{p}\right) = (-1)^{(\frac{p^2-1)}{8}}$. *Hence* 2 *is a quadratic residue of all primes* $p = \pm 1 (\bmod\ 8)$ *and a quadratic non residue of all primes* $p = \pm 3 (\bmod\ 8)$.

Proof. From Gauss Lemma we have $\left(\frac{2}{p}\right) = (-1)^i$ where i is the number of integers among $2 \cdot 1, 2 \cdot 2, 3 \cdot 2, \cdots (\frac{p-1}{2}) \cdot 2$ which have remainders greater than $\frac{p}{2}$ when divided by p. Here the integers $2j < \frac{p}{2}$ for $1 \leq i \leq \frac{p-1}{2}$ if and only if $j < \frac{p}{4}$. Hence there are $[\frac{p}{4}]$ integers which are less than $\frac{p}{2}$. Thus $i = \frac{p-1}{2} - [\frac{p}{4}]$ integers are greater than $\frac{p}{2}$. So by Gauss Lemma we have,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - [\frac{p}{4}]}.$$

To prove this we are to show,

$$\frac{p-1}{2} - [\frac{p}{4}] \equiv \frac{(p^2-1)}{8} (\bmod\ 2).$$

Consider congruence class modulo 8 as both sides of the above congruence depends only on the congruence class of p modulo 8. As p is an odd prime so p is of the forms $8j + 1,\ 8j + 3,\ 8j + 5,\ 8j + 7$. Now,

$$\text{if, } p = 8j + 1 \text{ then } i = 4j - \left[2j + \frac{1}{4}\right] = 4j - 2j = 2j$$

$$\text{if, } p = 8j + 3 \text{ then } i = 4j + 1 - \left[2j + \frac{3}{4}\right] = 4j + 1 - 2j = 2j + 1$$

$$\text{if, } p = 8j + 5 \text{ then } i = 4j + 2 - \left[2j + \frac{5}{4}\right] = 4j + 2 - 2j - 1 = 2j + 1$$

$$\text{if, } p = 8j + 7 \text{ then } i = 4j + 3 - \left[2j + \frac{7}{4}\right] = 4j + 3 - 2j - 1 = 2j + 2.$$

Thus, when $p = 8j+1$ or $p = 8j+7$ then i is even and $(\frac{2}{p}) = 1$; when $p = 8j+3$ or $p = 8j+5$ then i is odd and $(\frac{2}{p}) = -1$. So when $p \equiv \pm 1(\text{mod } 8)$ then 2 is a quadratic residue of all primes; when $p \equiv \pm 3(\text{mod } 8)$ then also 2 is a quadratic nonresidue of all primes. Now if $p \equiv \pm 1(\text{mod } 8)$ then $p = 8j \pm 1$ where j is an integer. So

$$\begin{aligned}\frac{p^2-1}{8} &= \frac{(8j\pm 1)^2-1}{8}\\ &= \frac{64j^2 \pm 16j}{8}\\ &= 8j^2 \pm 2j.\end{aligned}$$

Thu, in this case $\frac{p^2-1}{8}$ is even and $(-1)^{\frac{p^2-1}{8}} = 1 = (\frac{2}{p})$. Also, if $p \equiv \pm 3(\text{mod } 8)$ then $p = 8j \pm 3$ where j is an integer such that,

$$\begin{aligned}\frac{p^2-1}{8} &= \frac{(8j\pm 3)^2-1}{8}\\ &= \frac{64j^2 \pm 48j + 8}{8}\\ &= 8j^2 \pm 6j + 1.\end{aligned}$$

Thus, in this case $\frac{p^2-1}{8}$ is odd and $(-1)^{\frac{p^2-1}{8}} = -1 = (\frac{2}{p})$. Finally, for any odd prime p we find $(-1)^{\frac{p^2-1}{8}} = (\frac{2}{p})$. □

Example 9.2.5. *To exemplify the last theorem, pick out* $p = 23$ *for which* $(\frac{2}{23}) = (-1)^{\frac{23^2-1}{8}} = (-1)^{66} = 1$ *holds. Again, consider* $p = 11$ *such that* $(\frac{2}{11}) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1$.

Now, our next theorem directs another way of finding a primitive root. Because the proof of this theorem reflects some crucial applications of Legendre symbol, we include it in the present chapter instead of previous one.

Theorem 9.2.9. *Let* p *and* $2p+1$ *be two odd primes. Then the integer* $(-1)^{\frac{p-1}{2}} \cdot 2$ *is a primitive root of* $2p+1$.

Proof. We begin the proof by taking $q = 2p+1$. As p is an odd prime, then p is of the form $1+4k$ or $3+4k$ for any positive integer k. Hence

Case(i) $p = 1+4k$: Then $p \equiv 1(\text{mod } 4) \Rightarrow (-1)^{\frac{p-1}{2}} \cdot 2 = 2$. Since q is an odd prime and $\phi(q) = q-1 = 2p$ imply the order of 2 modulo p is one of $1, 2, p, 2p$. With the help of Euler's Criterion and Legendre symbol together we have, $(\frac{2}{q}) \equiv 2^{\frac{q-1}{2}} = 2^p(\text{mod } q)$. Now $p = 1+4k \Rightarrow q = 8k+3 \Rightarrow q \equiv 3(\text{mod } 8)$. In view of Theorem(9.2.8) we get, $(\frac{2}{q}) = -1$ which shows $2^p \equiv -1($

mod q). This concludes that p is not the order of 2 modulo q. Because $2^2 \equiv 1(\bmod q) \Rightarrow q|3$, is clearly impossible, the order of 2 is neither 1 nor 2. So the order of 2 modulo q is $2p$. This leads us to the fact that 2 becomes a primitive root modulo $q = 2p + 1$.

Case(ii) $p = 3 + 4k$: Then $p \equiv 3(\bmod 4) \Rightarrow (-1)^{\frac{p-1}{2}} \cdot 2 = -2$. Again, $p = 4k + 3 \Rightarrow q = 8k + 7 \Rightarrow q \equiv -1(\bmod 8)$. From Theorem 9.2.8 we have, $(\frac{2}{q}) = 1 \Rightarrow (-2)^p \equiv -1(\bmod p)$, since $(-2)^p \equiv (\frac{-2}{q}) = (\frac{-1}{q})(\frac{2}{q})(\bmod q)$ and $(\frac{-1}{q}) = -1$(refer to Theorem 9.2.4). Now, applying similar arguments as case(i), we can say that -2 is a primitive root of $q = 2p + 1$.

☐

For further illustration of this theorem, if we consider $p = 5$ then we can examine that 2 is a primitive root of $2p + 1 = 11$. Also for $p = 11$, -2 becomes the primitive root modulo $2p + 1 = 23$.

Before retiring from the field, we should mention another application of Legendre symbol on primes. The theorem here as follows.

Theorem 9.2.10. *There are infinitely many primes of the form* $8k - 1$.

Proof. To the contrary, suppose there are finitely many primes $p_1, p_2, \cdots p_n$. Let $T = (4p_1p_2\cdots p_n)^2 - 2$ and p be an odd prime divisor of T. This shows $4p_1p_2\cdots p_n$ is the solution of the equation $(4p_1p_2\cdots p_n)^2 \equiv 2(\bmod p)$. Thus $(\frac{2}{p}) = 1$ holds. Now, by Theorem 9.2.8 we have $p \equiv \pm 1(\bmod 8)$. If $p \equiv 1($ mod 8) then p is of the form $8k + 1$ which implies T of the form $16k' + 2$. This is impossible as T is of the form $16k' - 2$. Thus the prime divisor must be of the form $p' = 8k - 1$. Combining $p'|T$ and $p'|(4p_1p_2\cdots p_n)^2$ yields $p'|2$, a contradiction. So the number of primes of the form $8k - 1$ is infinite. ☐

9.3 Worked out Exercises

Problem 9.3.1. *For an odd prime p, prove that the quadratic residues modulo p are congruent modulo p to the integers*

$$1^2, 2^2, 3^2, \cdots, (\tfrac{p-1}{2})^2$$

Solution 9.3.1. *Let us take* $a = 1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$.
Then $a^{\frac{p-1}{2}} = 1^{p-1}, 2^{p-1}, \cdots (\frac{p-1}{2})^{p-1}$. *Now if we take* $b = 1, 2, 3, \cdots, \frac{p-1}{2}$, *then* $\gcd(b, p) = 1$ *as* $1 \leq b < p - 1$ *and p is a prime. By Fermat's Theorem, we have* $b^{p-1} \equiv 1(\bmod p)$. *This implies* $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$. *Applying Euler's Criterion, we can say that* $1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$ *are quadratic residue of p.*

Next we are to show $1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$ *incongruent modulo* p. *Let us choose* $a^2 \equiv b^2 (\bmod p)$, $1 \leq a, b \leq \frac{p-1}{2}$ *and* $a \neq b$. *Then we have* $(a+b)(a-b) \equiv 0(\bmod p)$. *Now* $a+b \leq \frac{p-1}{2} + \frac{p-1}{2} = p-1$, *implies* $\gcd(a+b, p) = 1$. *So we can divide both sides of the congruence by* $a+b$. *This shows that* $a - b \equiv 0(\bmod p)$. *Thus we have* $a \equiv b(\bmod p)$, *implies* $a = b$. *This is a contradiction.This shows that* $1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$ *are incongruent modulo* p.

Finally we have to show that any quadratic residue a *modulo* p *must be congruent to* $1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$. *Let* x_0 *be the solution of* $x^2 \equiv a(\bmod p)$ *where* $1 \leq x_0 \leq p-1$. *Here* $p - x_0$ *is also a solution. Then one of* x_0 *and* $p - x_0$ *must be less than or equal to* $p-1$. *Therefore one of* x_0^2 *or* $(p-x_0)^2$ *is equal to* $1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$. *Since* $x_0^2 \equiv a(\bmod p)$ *then we have,* $(p-x_0)^2 = p^2 - 2px_0 + x_0^2 \equiv a(\bmod p)$. *Thus* a *must be congruent to* $1^2, 2^2, 3^2, \cdots, (\frac{p-1}{2})^2$.

Problem 9.3.2. *Solve the following quadratic congruence:* $3x^2 + 9x + 7 \equiv 0(\bmod 13)$.

Solution 9.3.2. *To solve this, choose* $y = 2ax + b = 6x + 9$ *where* $a = 3$ *and* $b = 9$. *We transfer this equation in terms of* $y^2 \equiv d(\bmod 13)$, *where* $d = b^2 - 4ac = -3$. *This implies that* $y^2 \equiv -3 \equiv 10(\bmod 13)$. *Thus* $y \equiv 6, 7(\bmod 13)$. *Using* $y = 6x + 9$ *we see that,*

$$\begin{aligned} 6x + 9 &\equiv 6(\bmod 13) & \text{or, } 6x + 9 &\equiv 7(\bmod 13) \\ 6x &\equiv -3(\bmod 13) & 6x &\equiv -2(\bmod 13) \\ 6x &\equiv 36(\bmod 13) & 12x &\equiv -4(\bmod 13) \\ x &\equiv 6(\bmod 13) & x &\equiv 4(\bmod 13). \end{aligned}$$

Problem 9.3.3. *Prove that* 3 *is a quadratic residue of* 23.

Solution 9.3.3. *Here we have,* $3^{\frac{23-1}{2}} = 3^{11} = 9(27)^3$. *Then we can see that,*

$$\begin{aligned} 9(27)^3 &\equiv 9(4)^3(\bmod 23) \\ &\equiv 9 \cdot 64(\bmod 23) \\ &\equiv 9 \cdot (-5)(\bmod 23) \\ &\equiv 1(\bmod 23). \end{aligned}$$

By Euler's Criterion, we cay say that 3 *is a quadratic residue of* 23.

Problem 9.3.4. *Given that* a *is a quadratic residue of the odd prime* p, *prove that* $p - a$ *is a quadratic residue or nonresidue of* p *according as* $p \equiv 1(\bmod 4)$ *or* $p \equiv 3(\bmod 4)$.

Solution 9.3.4. *Here a is the quadratic residue modulo p. Then by Euler's Criterion we have, $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$. To verify $(p-a)$ is a quadratic residue or nonresidue, we need to consider $x^2 \equiv p-a \equiv -a(\bmod p)$. Thus either $(-a)^{\frac{p-1}{2}} \equiv 1(\bmod p)$ or $(-a)^{\frac{p-1}{2}} \equiv -1(\bmod p)$. But $(-a)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(\bmod p)$ implies that either $(-1)^{\frac{p-1}{2}} = 1$ or -1. This according as $\frac{p-1}{2}$ is even or odd .*

If $\frac{p-1}{2}$ is even, then $\frac{p-1}{2} = 2k$ for some integer k. This implies $p \equiv 1(\bmod 4)$.

If $\frac{p-1}{2}$ is odd, then $\frac{p-1}{2} = 2k'$ for some integer k'. This implies $p \equiv 3(\bmod 4)$.

Problem 9.3.5. *If $ab \equiv r(\bmod p)$, where r is the quadratic residue of the odd prime p, show that a and b are both quadratic residues of p or both nonresidues of p.*

Solution 9.3.5. *Here for $ab \equiv r(\bmod p)$ we have $\gcd(ab, p) = 1$. This implies that $\gcd(a, p) = 1$ and $\gcd(b, p) = 1$. Let us choose a as quadratic residue and b as quadratic nonresidue. Thus from the Corollary 9.2.1 we have $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$ and $b^{\frac{p-1}{2}} \equiv -1(\bmod p)$. This two together gives $r^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv -1(\bmod p)$. This shows r is a quadratic nonresidue. But this is not true. Since r is a quadratic residue then the possibilities are, $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1(\bmod p)$ or $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv -1(\bmod p)$. Thus a and b are both quadratic residues of p or both nonresidues of p.*

Problem 9.3.6. *If $p = 2^k + 1$ is a prime,show that every quadratic nonresidue of p is a primitive root of p.*

Solution 9.3.6. *Let a be a quadratic nonresidue modulo $p = 2^k + 1$. By Euler's Criterion we have, $a^{\frac{p-1}{2}} \equiv -1(\bmod p)$. As $2^k + 1$ is prime, then it implies $k \geq 1$ and $\frac{p-1}{2} = 2^{k-1}$. Therefore we have,*

$$a^{2^{k-1}} \equiv -1(\bmod p) \tag{9.3.1}$$

Note that $(a^{2^{k-1}})^2 = a^{2k} \equiv 1(\bmod p)$ and $\phi(p) = p - 1 = 2^k$. If n be the order of modulo p, then n must divide 2^k. Let $n = 2^r$ with $a^{2^r} \equiv 1(\bmod p)$ for some $r < k$. If $r = k - 1$, then (9.3.1) does not hold. This is a contradiction. If $r < k-1$, then $(a^{2^r})^2 = a^{2 \cdot 2^r} = a^{2^{r+1}} \equiv 1(\bmod p)$ and continuing this way after $(k-1) - r$ times we get, $a^{2^r} \equiv 1(\bmod p)$ which again contradicts (9.3.1). This shows that $n = 2^k = \phi(2^k+1)$, which implies a is a primitive root modulo 2^k+1.

Problem 9.3.7. *Find the value of the following Legendre symbol $(\frac{-72}{131})$.*

Solution 9.3.7. *Note that $(\frac{-72}{131}) = (\frac{-3^2 \cdot 2^2 \cdot 2}{131}) = (\frac{-1}{131})(\frac{2}{131})$ $[\because (\frac{a^2}{p}) = 1]$. However, by Euler's Criterion we have $(\frac{-1}{131}) = (-1)^{\frac{131-1}{2}} = -1$. Since $131 = 16 \cdot 8 + 3$,* *therefore by Theorem 9.2.8 we see that* $(\frac{2}{131}) = -1$. *These two together yields* $(\frac{-72}{131}) = (-1)(-1) = 1$.

Problem 9.3.8. *Use Gauss's lemma to compute the Legendre symbol* $(\frac{5}{19})$

Solution 9.3.8. *Note that* $p = 19$. *Then we can see that* $\frac{p-1}{2} = 9$ *and* $\frac{p}{2} = 9.5$, *which further yields* $S = \{5, 10, 15, 20, 25, 30, 35, 40, 45\} \equiv \{5, 10, 15, 1, 6, 11, 16, 2, 7\}(\bmod 19)$. *Thus the numbers* $10, 15, 16, 11$ *are greater than* 9.5. *So by Gauss Lemma we have for* $n = 4$, $(\frac{5}{19}) = (-1)^4 = 1$.

Problem 9.3.9. *Prove that* 2 *is not a primitive root of any prime of the form* $p = 3 \cdot 2^n + 1$, *except when* $p = 13$.

Solution 9.3.9. *To verify* 2 *is not a primitive root, its suffices to show that* 2 *is a quadratic residue of* p. *Now* $p - 1 = 3 \cdot 2^n$ *and by Theorem 9.2.8 we have,* $p - 1 \equiv 0(\bmod 8)$ *for* $n \geq 3$. *This shows that* $(\frac{2}{p}) = 1$ *and* 2 *is quadratic residue of* p.*Hence* 2 *is not a primitive root of* p.

Consider $n = 1$. *Then* $p = 3 \cdot 2 + 1 = 7$ *implies* $p \equiv 7(\bmod 8)$. *Moreover, by Theorem 9.2.8 we have* $(\frac{2}{p}) = 1$. *This shows that* 2 *is not a primitive root. If we consider* $n = 2$, *then* $p = 13$ *implies* $p \equiv 5(\bmod 8)$. *Again by virtue of Theorem 9.2.8, we have* $(\frac{2}{p}) = -1$. *So in this case,* 2 *is a quadratic non residue and hence a primitive root of* 13 *also.*

Problem 9.3.10. *For an odd prime p, show that there are* $\frac{p-1}{2} - \phi(p-1)$ *quadratic nonresidues of* p *that are not primitive roots of* p.

Solution 9.3.10. *In view of Theorem 9.2.6, we can say that there exist* $\frac{p-1}{2}$ *number of quadratic residues and non residues of* p.

Let a *be a quadratic residue of* p. *Then it can not be a primitive root because* $a^{\frac{p-1}{2}} \equiv 1(\bmod p)$*[by Corollary 9.2.1]. But* $\phi(p) = p - 1$ *implies* a *is not a primitive root. Thus if* r *is a primitive root of* p, *then it must be congruent to quadratic non residue of* p. *Let* S *be the set of quadratic non residue of* p. *Then* S *contains* $\frac{p-1}{2}$ *elements. From Corollary 8.2.3, there are* $\phi(p-1)$ *numbers of elements of* S *which are primitive roots of* p. *Thus* $[\frac{p-1}{2} - \phi(p-1)]$ *elements of* S *are not primitive roots of* p.

Problem 9.3.11. *If* p *is an odd prime, prove that*

$$\sum_{a=1}^{p-2} (\frac{a(a+1)}{p}) = -1.$$

Solution 9.3.11. *Let us choose an integer* a *such that* $\gcd(a, p) = 1$. *Then from linear congruence we can say that there exists an integer* a' *satisfying* $aa' \equiv 1(\bmod p)$ *for* $1 \leq a \leq p - 2$.

Here both a and a' *runs from* 1 *to* $p-2$. *However if* $a' = p-1$, *then* $a(p-1) \equiv 1(\bmod p)$. *This implies* $-a \equiv 1(\bmod p) \Rightarrow a+1 \equiv 0(\bmod p)$, *which shows that* $p-1 = a$, *a contradiction.*

Let $a_1 a' \equiv 1(\bmod p)$ *and* $a_2 a' \equiv 1(\bmod p)$. *Then* $a_1 a' \equiv a_2 a'(\bmod p)$ *implies* $a_1 = a_2$. *This shows that if a runs from* 1 *to* $p-2$, *then each* a' *from* 1 *to* $p-2$ *is represented only once. As a runs from* 1 *to* $p-2$, *so* $1+a'$ *runs from* 2 *to* $p-1$.

$$\begin{aligned}
&\therefore aa' \equiv 1(\bmod p)\\
&\Rightarrow a + aa' \equiv a+1(\bmod p)\\
&\Rightarrow a(1+a') \equiv a+1(\bmod p)\\
&\Rightarrow a^2(a'+1) \equiv a(a+1)(\bmod p).
\end{aligned}$$

Thus we have, $\left(\frac{a(a+1)}{p}\right) = \left(\frac{a^2(a'+1)}{p}\right) = \left(\frac{1+a'}{p}\right)$. *Now we can see that,*

$$\begin{aligned}
\sum_{a=1}^{p-2}\left(\frac{a(a+1)}{p}\right) &= \sum_{1+a'=2}^{p-2}\left(\frac{1+a'}{p}\right)\\
&= \sum_{a'=2}^{p-1}\left(\frac{a'}{p}\right)\\
&= \sum_{a=2}^{p-1}\left(\frac{a}{p}\right)\\
&= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) - \left(\frac{1}{p}\right).
\end{aligned}$$

By Theorem 9.2.6we have, $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$ *and* $\left(\frac{1}{p}\right) = 1$. *This proves* $\sum_{a=1}^{p-2}\left(\frac{a(a+1)}{p}\right) = -1$.

Problem 9.3.12. *If* $p \equiv 7(\bmod 8)$, *then prove that* $p | 2^{\frac{p-1}{2}} - 1$. *Hence show that* $2^n - 1$ *is composite for* $n = 239$

Solution 9.3.12. *From Euler's Criterion we have,* $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}(\bmod p)$. *Moreover, since* $p \equiv 7(\bmod 8)$ *therefore by Theorem 9.2.8 we have* $\left(\frac{2}{p}\right) = 1$. *Thus together we say that* $2^{\frac{p-1}{2}} - 1 \equiv 0(\bmod p)$. *Hence* $p \big| \left(2^{\frac{p-1}{2}} - 1\right)$.

For the remaining part, to verify $2^{239} - 1$ *is composite, we need to express* 239 *as* $\frac{p-1}{2}$ *for some p of the form* $7 + 8k (k \in \mathbb{Z})$. *Hence* $239 = \frac{p-1}{2} \Rightarrow p = 503 = 7 + 62 \cdot 8$.

Problem 9.3.13. *If the prime* $p > 3$, *prove that p divides the sum of its quadratic residues.*

Solution 9.3.13. *Let* r *be a primitive root modulo* p *and* $a_1, a_2, \cdots, a_{\frac{p-1}{2}}$ *be the quadratic residue of* p*. By Corollary 9.2.2,* $r^2, r^4, \cdots r^{p-1}$ *are congruent to the quadratic residue of* p*. Therefore*

$$\begin{aligned} a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} &\equiv r^2 + r^4 + \cdots r^{p-1} (\bmod p) \\ &\equiv r^2(1 + r^2 + r^4 + \cdots r^{p-3}) (\bmod p) \; [\because p > 3]. \end{aligned}$$

Since r *is a primitive root, so* $r^{p-1} \equiv 1(\bmod p)$*. Therefore,*

$$\begin{aligned} a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} &\equiv r^2 + r^4 + \cdots r^{p-3} + r^{p-1} (\bmod p) \\ \Rightarrow a_1 + a_2 + \cdots + a_{\frac{p-1}{2}} &\equiv (1 + r^2 + r^4 + \cdots r^{p-3}) (\bmod p). \end{aligned}$$

Now from the above two congruence equation for $p > 3$ *we have,*

$$r^2(1 + r^2 + r^4 + \cdots r^{p-3}) \equiv (1 + r^2 + r^4 + \cdots r^{p-3}) (\bmod p).$$

Here p *must divide* $(1 + r^2 + r^4 + \cdots r^{p-3})$*, otherwise* $r^2 \equiv 1(\bmod p)$ *which contradicts the fact that* r *is primitive root as* $p > 3$*. Thus we have,* $p | (a_1 + a_2 + \cdots + a_{\frac{p-1}{2}})$*.*

Problem 9.3.14. *Show that the odd prime divisor* p *of the integers* $9^n + 1$ *are of the form* $p \equiv 1(\bmod 4)$*.*

Solution 9.3.14. *Here* p *is an odd prime divisor of* $9^n + 1$*. Then* $9^n + 1 \equiv 0(\bmod p)$ *or* $(3^n)^2 \equiv -1(\bmod p)$*. Since* p *is odd, therefore either* $p \equiv 1(\bmod 4)$ *or* $p \equiv 3(\bmod 4)$*. Now by Theorem 9.2.4, if* $p \equiv 3(\bmod 4)$ *we can say that there does not exists any solution of* $x^2 \equiv -1(\bmod p)$*. So there is no solution of* $(3^n)^2 \equiv -1(\bmod p)$*. Thus* p *is the divisor of* $9^n + 1$ *if it must be of the form* $p \equiv 1(\bmod 4)$*.*

9.4 Quadratic Reciprocity Law

Here in this section we have discussed another important of modular arithmetic which gives us the path to solve quadratic congruences modulo prime numbers. If we choose two odd primes p and q then both the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are defined. A fairly question presents itself: Is it possible to find any one of them with the help of other. The answer is contained in the notion 'Quadratic Reciprocity Law': $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)\frac{p-1}{2} \cdot \frac{q-1}{2}$. Also, this leads to the fact that if $x^2 \equiv p(\bmod q)$ is solvable then $x^2 \equiv q(\bmod p)$ is also so and vice versa. Now before going to the proof of above quadratic reciprocity law we have to prove a significant lemma first. This lemma further leads us to prove this important law of modular arithmetic.

Lemma 9.4.1. *If p is an odd prime and r is an odd integer with* $\gcd(r,p)=1$ *then* $\left(\dfrac{r}{p}\right)=(-1)^{\sum_{t=1}^{\frac{p-1}{2}}[tr/p]}$.

Proof. To begin with, consider the integers $r, 2r, \cdots (\dfrac{p-1}{2})r$ among which some are greater than $\frac{p}{2}$ and the rest are less than $\frac{p}{2}$ when divided by p. Let $r_1, r_2, \cdots r_n$ be the remainders less than $\frac{p}{2}$ and $s_1, s_2, \cdots s_m$ be the remainders greater than $\frac{p}{2}$. Dividing every element of $r, 2r, \cdots (\dfrac{p-1}{2})r$ by p we get, $tr = q_t p + w_t$ where $1 \leq w_t \leq p-1$. Then $\frac{tr}{p} = q_t + \frac{w_t}{p} \Rightarrow q_t = [tr/p]$ for $1 \leq t \leq \frac{p-1}{2}$. Hence $tr = [tr/p]p + w_t$.

If the remainder $w_t < \frac{p}{2}$, it is one of $r_1, r_2, \cdots r_n$ and if $w_t > \frac{p}{2}$ then it is one of $s_1, s_2, \cdots s_m$. Adding both sides of the last equation we have,

$$\sum_{t=1}^{\frac{p-1}{2}} tr = \sum_{t=1}^{\frac{p-1}{2}} [tr/p]\cdot p + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j \tag{9.4.1}$$

Taking the proof of Gauss Lemma into consideration, the integers $r_1, r_2, \cdots r_n, p-s_1, p-s_2, \cdots p-s_m$ are among $1, 2, \cdots \frac{p-1}{2}$ in some order. Therefore

$$\sum_{t=1}^{\frac{p-1}{2}} t = \sum_{i=1}^{n} r_i + \sum_{j=1}^{m}(p-s_j) = pm + \sum_{i=1}^{n} r_i - \sum_{j=1}^{m} s_j \tag{9.4.2}$$

Subtracting (9.4.2) from (9.4.1)we get,

$$(r-1)\sum_{t=1}^{\frac{p-1}{2}} t = p(\sum_{t=1}^{\frac{p-1}{2}}[tr/p] - m) + 2\sum_{j=1}^{m} s_j \tag{9.4.3}$$

As p and r are both odd, the application of $p \equiv r \equiv 1(\text{mod } 2)$ on (9.4.3) tells us,

$$0\cdot\sum_{t=1}^{\frac{p-1}{2}} t \equiv 1\cdot(\sum_{t=1}^{\frac{p-1}{2}}[tr/p] - m)(\text{ mod } 2) \Rightarrow m \equiv \sum_{t=1}^{\frac{p-1}{2}}[tr/p](\text{ mod } 2). \tag{9.4.4}$$

Finally, Gauss Lemma leads us to conclude that $(\frac{r}{p}) = (-1)^m = (-1)^{\sum_{t=1}^{\frac{p-1}{2}}[tr/p]}$.

□

The above lemma is not only a tool to prove quadratic reciprocity law but also used to evaluate Legendre symbol. For instance, if we wish to prove $(\frac{5}{11})$, by above lemma we only need to evaluate $\sum_{t=1}^{\frac{11-1}{2}}[t\cdot 5/11]$.

Here,

$$\sum_{t=1}^{5}[t\cdot 5/11]=[5/11]+[10/11]+[15/11]+[20/11]+[25/11]=0+0+1+1+2=4.$$

Hence $(\frac{5}{11})=(-1)^4=1$. Now, the actual details of the Gauss Quadratic Reciprocity Law appear below.

Theorem 9.4.1. *If p and q are distinct odd primes, then* $(\frac{p}{q})(\frac{q}{p})=(-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$.

Proof. To start with, consider a pair of integers (x,y) with $1\le x\le\frac{p-1}{2}$ and $1\le y\le\frac{q-1}{2}$. Now we divide the total number of pair $(\frac{p-1}{2})(\frac{q-1}{2})$ into two groups, which depends on the relative sizes of qx and py. Geometrically it can be interpreted by a diagonal of a rectangle from $(0,0)$ to $(\frac{p}{2},\frac{q}{2})$ as shown in the figure below:

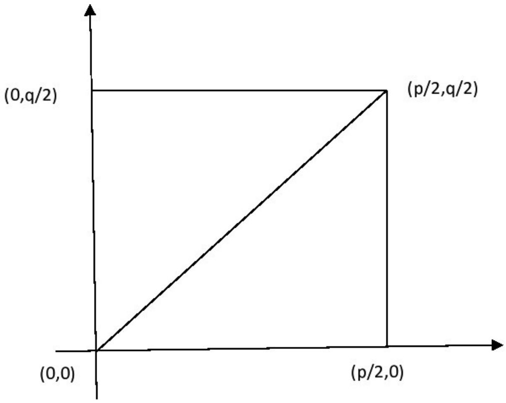


Figure 9.1:

Here the equation of the diagonal is $y=(\frac{q}{p})x$, with slope $\frac{q}{p}$. First, we wish to ensure that the pair do not coincide with the diagonal. If so, then $py=qx\Rightarrow q|py$. Then either $q|p$ or $q|y$ holds. Since $\gcd(p,q)=1$ so $q\nmid p$. Also $1\le y\le\frac{q-1}{2}$ implies $q\nmid y$. Thus, $py=qx$ is not possible.

Let $qx > py$. Then we have, $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{qx}{p}$. So for each x lying between 1 and $\frac{p-1}{2}$, there are $[qx/p]$ number of integers satisfying $1 \leq y \leq \frac{qx}{p}$. So the total number of such pair are $\sum_{i=1}^{\frac{p-1}{2}} [qi/p]$.

Again, if $qx < py$ then $1 \leq y \leq \frac{q-1}{2}$ and $1 \leq x \leq \frac{py}{q}$. Proceeding as above, the total number of such pair are $\sum_{j=1}^{\frac{q-1}{2}} [pj/q]$. As the total number of coordinates in x and y are $\frac{p-1}{2} \cdot \frac{q-1}{2}$, therefore $\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{\frac{p-1}{2}} [qi/p] + \sum_{i=1}^{\frac{p-1}{2}} [qi/p]$. Appealing to Lemma 9.4.1 we get,

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\sum_{j=1}^{\frac{q-1}{2}} [pj/q]} \times (-1)^{\sum_{i=1}^{\frac{p-1}{2}} [qi/p]} \\ &= (-1)^{\sum_{j=1}^{\frac{q-1}{2}} [pj/q] + \sum_{i=1}^{\frac{p-1}{2}} [qi/p]} \\ &= (-1)^{(\frac{p-1}{2}) \cdot (\frac{q-1}{2})}.\end{aligned}$$

This proves the law of quadratic reciprocity. □

Corollary 9.4.1. *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv 1(\mod 4) \textit{ or } q \equiv 1(\mod 4); \\ -1, & \textit{if } p \equiv q \equiv 3(\mod 4). \end{cases}$$

Proof. As $(\frac{p}{q})(\frac{q}{p}) = (-1)^{(\frac{p-1}{2}) \cdot (\frac{q-1}{2})}$, then the number $(\frac{p-1}{2}) \cdot (\frac{q-1}{2})$ is even if and only if at least one of them is of the form $4j + 1$ for some integer j. This shows that $p \equiv 1(\text{mod } 4)$ or $q \equiv 1(\text{mod } 4)$. Also $(\frac{p-1}{2}) \cdot (\frac{q-1}{2})$ is odd if and only if both p and q are of the form $4j + 3$ for some integer j, which further implies $p \equiv q \equiv 3(\text{mod } 4)$. Our task is complete. □

The above corollary gives birth to the following obvious corollary.

Corollary 9.4.2. *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}), & \textit{if } p \equiv 1(\mod 4) \textit{ or } q \equiv 1(\mod 4); \\ -(\frac{q}{p}), & \textit{if } p \equiv q \equiv 3(\mod 4). \end{cases}$$

For example, if we consider the Legendre symbols $(\frac{5}{11})$ and $(\frac{11}{5})$ then Theorem (9.4.1) yields,

$$\begin{aligned}\left(\frac{5}{11}\right)\left(\frac{11}{5}\right) &= (-1)^{\frac{5-1}{2} \cdot \frac{11-1}{2}} \\ &= (-1)^{10} = 1\end{aligned}$$

Thus, according to the last corollary we have $(\frac{11}{5}) = (\frac{5}{11}) = 1$.

Finally, we conclude this section with the following theorem.

Theorem 9.4.2. *If $p \neq 3$ is an odd prime, then*

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv \pm 1(\mod 12) \\ -1, & \textit{if } p \equiv \pm 5(\mod 12). \end{cases}$$

Proof. Appealing to Corollary(9.4.2) we get,

$$\left(\frac{3}{p}\right) = \begin{cases} (\frac{p}{3}), & \text{if } p \equiv 1(\mod 4) \\ -(\frac{p}{3}), & \text{if } p \equiv -1(\mod 4). \end{cases}$$

Set $p \equiv 1(\text{mod } 3)$. Recalling Theorem 9.2.3 we get $(\frac{p}{3}) = (\frac{1}{3}) = 1$. Also, if $p \equiv -1(\mod 3)$ then by similar reasoning we have, $(\frac{p}{3}) = (\frac{-1}{3})$ and $(\frac{-1}{3}) \equiv (-1)^{\frac{3-1}{2}}(\mod 3)$. Combining we get $(\frac{p}{3}) = -1$. Thus,

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{if } p \equiv 1(\mod 3) \\ -1, & \text{if } p \equiv -1(\mod 3). \end{cases}$$

Combining $p \equiv 1(\text{mod } 4)$ and $p \equiv 1(\text{mod } 3)$ yield $p \equiv 1(\text{mod } 12)$(Why!). Also, $p \equiv -1(\text{mod } 4)$ and $p \equiv -1(\text{mod } 3)$ together gives $p \equiv -1(\text{mod } 12)$.

Suppose $p \equiv 1(\text{mod } 4)$ and $p \equiv -1(\text{mod } 3)$. Then for $z, z' \in \mathbb{Z}$ we have $p - 1 = 4z$, $p + 1 = 3z'$. On solving, we get $p + 7 = 12(z' - z)$ which implies $p \equiv -7 \equiv 5(\text{mod } 12)$. Finally, for $p \equiv -1(\text{mod } 4)$ and $p \equiv 1(\text{mod } 3)$ there exist integers t, t' such that $p + 1 = 4t$ and $p - 1 = 3t'$. Proceeding as above, we get $p \equiv 7 \equiv -5(\text{mod } 12)$. This leads us to,

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1(\mod 12) \\ -1, & \text{if } p \equiv \pm 5(\mod 12). \end{cases}$$

□

9.5 Worked out Exercises

Problem 9.5.1. *Evaluate the following Legendre symbol:* $(\frac{1234}{4567})$.

Solution 9.5.1. *Here* $4567 \equiv 3(\text{mod } 4)$ *and* $1234 = 2 \cdot 617$. *Also* $617 \equiv 1($

mod 4). *An appeal to Theorem 9.2.8 and Corollary 9.4.2) yields*

$$\begin{aligned}\left(\frac{1234}{4567}\right) &= \left(\frac{2}{4567}\right)\left(\frac{617}{4567}\right) = \left(\frac{4567}{617}\right)[\because,\ 4567 \equiv 7(\mod 8)]\\ &= \left(\frac{248}{617}\right) = \left(\frac{2}{617}\right)\left(\frac{31}{617}\right)[\because, 248 = 2^3 \cdot 31]\\ &= \left(\frac{31}{617}\right) = \left(\frac{617}{31}\right) = \left(\frac{28}{31}\right)\\ &= \left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right)\\ &= \left(\frac{1}{3}\right) = 1.\end{aligned}$$

Problem 9.5.2. *Show that if p is an odd prime, then*

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv 1(\mod 8) \textit{ or } p \equiv 3(\mod 8)\\ -1, & \textit{if } p \equiv 5(\mod 8) \textit{ or } p \equiv 7(\mod 8).\end{cases}$$

Solution 9.5.2. *Note that* $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$. *By Theorem 9.2.4, we can say that* $(\frac{-1}{p}) = 1$ *if* $p \equiv 1(\mod 4)$ *and by Theorem 9.2.8 we have* $(\frac{2}{p}) = 1$ *if* $p \equiv \pm1(\mod 8)$. *By similar arguments,* $(\frac{-1}{p}) = -1$ *if* $p \equiv 3(\mod 4)$ *and* $(\frac{2}{p}) = -1$ *if* $p \equiv \pm3(\mod 8)$. *However if* $p \equiv 1(\mod 8)$, *then* $p \equiv 1(\mod 4)$ *which gives* $(\frac{-2}{p}) = 1$. *Furthermore if* $p \equiv 3(\mod 8)$, *then* $p \equiv 3(\mod 4)$. *Thus* $(\frac{-2}{p}) = (-1)\cdot(-1) = 1$. *Moreover if* $p \equiv -3 \equiv 5(\mod 8)$, *then* $p \equiv 5 \equiv 1(\mod 4)$, *which shows* $(\frac{-2}{p}) = (-1)\cdot 1 = -1$. *Also if* $p \equiv 7(\mod 8)$, *then* $p \equiv 7 \equiv 3(\mod 4)$ *shows* $(\frac{-2}{p}) = (1)\cdot(-1) = -1$. *Combining all those results we obtain,*

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \textit{if } p \equiv 1(\mod 8) \textit{ or } p \equiv 3(\mod 8)\\ -1, & \textit{if } p \equiv 5(\mod 8) \textit{ or } p \equiv 7(\mod 8)\end{cases}$$

Problem 9.5.3. *Determine whether the following quadratic congruence is solvable or not:* $3x^2 + 6x + 5 \equiv 0(\mod 89)$.

Solution 9.5.3. *Let us consider the equation* $3x^2 + 6x + 5 \equiv 0(\mod 89)$. *So*

$$\begin{aligned}&3x^2 + 6x + 5 \equiv 0(\mod 89)\\ \Rightarrow\ &(6x+6)^2 + 24 \equiv 0(\mod 89)\\ \Rightarrow\ &(6x+6)^2 \equiv 65(\mod 89).\end{aligned}$$

Let $y = 6x + 6$. *Then* $y^2 \equiv 65(\mod 89)$. *As* $13 \equiv 1(\mod 4)$, *then by Corollary 9.4.2) we can write,*

$$\left(\frac{13}{89}\right) = \left(\frac{89}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1[\textit{Since } 11 \equiv 3(\mod 8)]$$

Moreover $5 \equiv 1(\bmod 4)$. *Then by Corollary 9.4.2 we can say that,*

$$\left(\frac{5}{89}\right) = \left(\frac{89}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$$

Together we have, $\frac{65}{89} = -1$. *This shows that the given equation is not solvable.*

Problem 9.5.4. *Verify that if* $p > 3$ *is an odd prime, then*

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1(\bmod 6) \\ -1, & \text{if } p \equiv 5(\bmod 6) \end{cases}$$

Solution 9.5.4. *Let us take* $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p})$. *To prove the assertion we are to consider two cases:*

Case(i): *Let* $p \equiv 1(\bmod 6)$. *Then* $p - 1 = 6t$ *for some integer* $t(> 0)$.

1. *If* t *is even, then* $t = 2t'$ *for some integer* $t'(> 0)$. *This shows that* $p - 1 = 12t'$ *or* $p \equiv 1(\bmod 12)$. *Therefore* $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{6t'} = 1$ *and* $(\frac{3}{p}) = 1$*[by Theorem 9.4.2]. Therefore* $(\frac{-3}{p}) = 1$.
2. *If* t *is odd, then* $t = 2t' + 1$. *This shows that* $p - 1 = 6(2t' + 1)$ *or* $p \equiv 7 \equiv -5(\bmod 12)$. *Therefore* $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{3+6t'} = -1$. *Then by Theorem 9.4.2 we have* $(\frac{-3}{p}) = 1$. *Hence* $p \equiv 1(\bmod 6) \Rightarrow (\frac{-3}{p}) = 1$.

Case(ii): *Let* $p \equiv 5(\bmod 6)$. *Then* $p - 5 = 6k$ *for some integer* $k(> 0)$.

1. *If* k *is even, then* $t = 2k'$ *for some integer* $k'(> 0)$. *This shows that* $p - k = 12k'$ *or* $p \equiv 5(\bmod 12)$. *Therefore* $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{2+6k'} = 1$ *and* $(\frac{3}{p}) = -1$*[by Theorem 9.4.2]. Therefore* $(\frac{-3}{p}) = -1$.
2. *If* k *is odd, then* $t = 2k' + 1$. *This shows that* $p - 5 = 6(2k' + 1)$ *or* $p \equiv -1(\bmod 12)$. *Therefore* $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{5+6t'} = -1$. *Then by Theorem 9.4.2 we have* $(\frac{-3}{p}) = -1$. *Therefore* $p \equiv 5(\bmod 6) \Rightarrow (\frac{-3}{p}) = -1$.

Problem 9.5.5. *Prove that there exist infinitely many primes of the form* $8k+3$.

Solution 9.5.5. *To the contrary, let us assume that there exists finitely many primes of the form* $8k + 3$ *say,* $p_1, p_2, \cdots, p_n$. *Consider* $M = (p_1 p_2 \cdots p_n)^2 + 2$. *Then* M *is odd and it has an odd prime divisor* p *such that* $p \neq p_i$. *For if* $p = p_i$, *then* $p|M$ *and* $p|(p_1 p_2 \cdots p_n)^2$ *together imply* $p|2$.

Now $M \equiv 0(\bmod p)$ *imply* $(p_1 p_2 \cdots p_n)^2 \equiv -2(\bmod p)$. *So either* $p \equiv 1(\bmod 8)$ *or* $p \equiv 3(\bmod 8)$*[refer to Problem 9.5.2]. Let* $M = q_1^{k_1} q_2^{k_2} \cdots q_s^{k_s}$ *and*

$q_i \equiv 1 (\mathrm{mod}\ 8)$ for all i. But $p_i \equiv 3(\mathrm{mod}\ 8)$ imply $p_i^2 \equiv 9 \equiv 1(\mathrm{mod}\ 8)$. This shows that $(p_1p_2\cdots p_n)^2+2 \equiv 3(\mathrm{mod}\ 8)$ i.e. $M \equiv 3(\mathrm{mod}\ 8)$, a contradiction to the fact that $M = q_1^{k_1}q_2^{k_2}\cdots q_s^{k_s} \equiv 1(\mathrm{mod}\ 8)$.

Therefore all q_i's can't be of the form $q_i \equiv 1(\mathrm{mod}\ 8)$. So there must be some odd prime divisor $q_i = p$ of M such that $p \equiv 3(\mathrm{mod}\ 8)$. This contradicts the fact that p_i's are finite.

Problem 9.5.6. *Show that $(\frac{5}{p}) = 1$ if and only if $p \equiv 1, 9, 11, 19(\mathrm{mod}\ 20)$.*

Solution 9.5.6. *By definition of Legendre symbol, we have p is an odd prime. If $p \equiv 1, 9, 11, 19(\mathrm{mod}\ 20)$, then we have $p \equiv 1, 9, 11, 19(\mathrm{mod}\ 5)$. This shows that $p \equiv 1, 4(\mathrm{mod}\ 5)$. As $5 \equiv 1(\mathrm{mod}\ 4)$, by Corollary 9.4.2 we find $(\frac{5}{p}) = (\frac{p}{5}) = (\frac{1}{5})$ or$(\frac{4}{5})$. In any case $(\frac{5}{p}) = 1$.*

For the converse part, let $(\frac{5}{p}) = 1$ holds. Since $5 \equiv 1(\mathrm{mod}\ 4)$, therefore $(\frac{5}{p}) = (\frac{p}{5}) = 1$. So by Euler's Criterion, $p^{\frac{5-1}{2}} \equiv 1(\mathrm{mod}\ 5)$ yields $p \equiv 1,\ 4(\mathrm{mod}\ 5)$. Furthermore, for an odd prime we have $p \equiv 1,\ 3(\mathrm{mod}\ 4)$. Those above congruences imply that $4p \equiv 4(\mathrm{mod}\ 20)$ or $4p \equiv 16(\mathrm{mod}\ 20)$ and also $5p \equiv 5(\mathrm{mod}\ 20)$ or $5p \equiv 15(\mathrm{mod}\ 20)$. Subtracting them we get, $p \equiv -1 or\ 11(\mathrm{mod}\ 20)$. This follows that $p \equiv 1, 9, 11, 19(\mathrm{mod}\ 20)$.

Problem 9.5.7. *If p and q are odd primes satisfying $p = q+4a$ for some integer a, prove that $(\frac{a}{p}) = (\frac{a}{q})$.*

Solution 9.5.7. *Since $p = q+4a$, therefore $(\frac{p}{q}) = (\frac{q+4a}{q})$. But $q+4a \equiv 4a(\mathrm{mod}\ q)$. Thus $(\frac{p}{q}) = (\frac{4a}{q}) = (\frac{a}{q})$. Similarly, $q = p-4a$ implies $(\frac{q}{p}) = (\frac{-a}{p}) = (\frac{-1}{p})(\frac{a}{p})$. As p is odd, two cases arise:*

Case(i): If $p \equiv 1(\mathrm{mod}\ 4)$, then Theorem 9.2.4 yields $(\frac{-1}{p}) = 1$. So $(\frac{q}{p}) = (\frac{a}{p})$. By Corollary 9.4.2, we find $(\frac{q}{p}) = (\frac{p}{q})$ as $p \equiv 1(\mathrm{mod}\ 4)$. Then applying all above notions we get, $(\frac{a}{p}) = (\frac{a}{q})$.

Case(ii): If $p \equiv 3(\mathrm{mod}\ 4)$, then by Theorem 9.2.4 we have $(\frac{-1}{p}) = -1$. Thus we get $(\frac{q}{p}) = -(\frac{a}{p})$. As $p = q+4a$, then $p \equiv q(\mathrm{mod}\ 4)$ implies $q \equiv 3(\mathrm{mod}\ 4)$. Moreover, by Corollary 9.4.2 we have $(\frac{q}{p}) = -(\frac{p}{q})$. In this case we can say that $(\frac{a}{q}) = -(\frac{q}{p}) = (\frac{a}{p})$.

Problem 9.5.8. *Find a prime number p that is simultaneously expressible in the forms x^2+y^2, u^2+2v^2 and r^2+3s^2.*

Solution 9.5.8. *Let us take $x^2+y^2 = p$. Then $\frac{x^2}{y^2} \equiv -1(\mathrm{mod}\ p)$. Similarly $\frac{u^2}{v^2} \equiv -2(\mathrm{mod}\ p)$ and $\frac{r^2}{s^2} \equiv -3(\mathrm{mod}\ p)$. To find the value of p we need to apply the condition $(\frac{-1}{p}) = (\frac{-2}{p}) = (\frac{-3}{p}) = 1$.*

Therefore for $(\frac{-1}{p}) = 1$, *we get* $p \equiv 1(\bmod 4)$. *Similarly, we get* $(\frac{-2}{p}) = 1$ *provided* $p \equiv 1(\bmod 8)$ *or* $p \equiv 3(\bmod 8)$. *However, if* $p \equiv 1(\bmod 6)$ *then* $(\frac{-3}{p}) = 1$.

If $p \equiv 1(\bmod 24)$, *then* $p \equiv 1(\bmod 4)$, $p \equiv 1(\bmod 8)$ *and* $p \equiv 1(\bmod 6)$ *holds together. Let us consider* $p = 1 + 24k$ *for* $k = 1, 2, 3 \cdots$. *Then* $p = 25, 49, 73, \cdots$. *In particular,* 73 *is a prime and it can be written as* $8^2 + 3^2 = 73 = 1^2 + 2(6)^2 = 5^2 + 3(4)^2$.

Problem 9.5.9. *Show that the prime divisors* $p(\neq 3)$ *of the integer* $n^2 - n + 1$ *are of the form* $6k + 1$.

Solution 9.5.9. *Note that* $n^2 - n + 1$ *is odd for all* $n \geq 1$*(Verify!). If* p *is a prime divisor of* $n^2 - n + 1$, *then* $p > 3$ *as* $n^2 - n + 1 \neq 2$ *and* $p \neq 3$. *If* $p | n^2 - n + 1$, *then* p *also divides* $(2n - 1)^2 + 3$. *Therefore* $(2n-1)^2 \equiv -3(\bmod p)$ *follows that* $(\frac{-3}{p}) = 1$. *This shows that* $p \equiv 0, 1, 2, 3, 4, 5(\bmod 6)$. *If* $p = 0, 2, 4 \equiv (\bmod 6)$, *then we have* $p \equiv 0, 2, 4(\bmod 2)$, *which is not possible as* $p > 3$. *If* $p \equiv 3(\bmod 6)$, *then* $p \equiv 3(\bmod 6)$ *implies* $3|p$, *a contradiction as* $p > 3$. *Thus for* $p \equiv 5(\bmod 6)$ *we have* $(\frac{-3}{p}) = -1$ *[by Problem 9.5.4]. This shows that* $p \equiv 1(\bmod 6)$ *holds and* p *is of the form* $1 + 6k$ *for some integer* k.

9.6 The Jacobi Symbol

In this section, we conduct a study on another important symbol of number theory known as Jacobi symbol. This is the generalization of Legendre symbol studied in previous section. The symbol acts as an utilitarian in evaluating Legendre symbol.

Definition 9.6.1. *Let* n *be a positive integer and* $n = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$ *be its prime factorization where each* p_i*'s are distinct. Then the Jacobi symbol* $\left(\frac{r}{n}\right)$ *is defined by* $\left(\frac{r}{n}\right) = \left(\frac{r}{p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}}\right) = \left(\frac{r}{p_1}\right)^{n_1} \left(\frac{r}{p_2}\right)^{n_2} \cdots \left(\frac{r}{p_n}\right)^{n_m}$, r *being any positive integer relatively prime to* n. *Here the symbols* $\left(\frac{r}{p_i}\right)$ *for each* $i = 1, 2, \cdots m$ *are known to be Legendre symbol.*

To illustrate, let us choose $a = 2$, $b = 147$. Then $\left(\frac{2}{147}\right) = \left(\frac{2}{7^2 \cdot 3}\right) = \left(\frac{2}{7}\right)^2 \left(\frac{2}{3}\right) = (-1)(-1)^2 = -1$.

This demonstrates, in particular, Jacobi symbol is Legendre symbol if n is prime. However for any composite number n, the value of $\left(\frac{r}{n}\right)$ fails to assure the solvability of the congruence $x^2 \equiv r(\bmod p)$. Since $x^2 \equiv 3(\bmod 5)$ and $x^2 \equiv (\bmod 7)$ have no solutions, therefore the equation $x^2 \equiv 3(\bmod 5)$ has no solution. Although we can see that $\left(\frac{3}{35}\right) = \left(\frac{3}{5}\right)\left(\frac{3}{7}\right) = (-1)(-1) = 1$. Thus for any composite integer n and any prime divisor p of n, $x^2 \equiv r(\text{mod } n)$ has a solution if $x^2 \equiv r(\text{mod } p)$ is solvable.

Jacobi symbol also relish certain interchangeable properties to those of the Legendre symbol.

Theorem 9.6.1. *Let n be a composite number and r, s be integers such that* $\gcd(r, n) = 1$ *and* $\gcd(s, n) = 1$ *respectively. Then the following properties are true:*

1. *If $r \equiv s(\text{mod } n)$ then $(\frac{r}{n}) = (\frac{s}{n})$.*
2. $\left(\frac{r}{n}\right)\left(\frac{s}{n}\right) = \left(\frac{rs}{n}\right)$.
3. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.
4. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Proof. To prove these four assertions, consider $n = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$ to be its prime factorization.

1. Let p be the prime divisor of n. Then $r \equiv s(\text{mod } p)$ holds. Taking Theorem 9.2.3 into consideration, we obtain $\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right)$. This implies,

$$\begin{aligned}\left(\frac{r}{n}\right) &= \left(\frac{r}{p_1}\right)^{n_1}\left(\frac{r}{p_2}\right)^{n_2}\cdots\left(\frac{r}{p_n}\right)^{n_m}\\ &= \left(\frac{s}{p_1}\right)^{n_1}\left(\frac{s}{p_2}\right)^{n_2}\cdots\left(\frac{s}{p_n}\right)^{n_m}\\ &= \left(\frac{s}{n}\right).\end{aligned}$$

2. Again, by Theorem 9.2.3 we find $\left(\frac{rs}{p_i}\right) = \left(\frac{r}{p_i}\right)\left(\frac{s}{p_i}\right)$ for each i. Thus we can deduce that,

$$\begin{aligned}\left(\frac{rs}{n}\right) &= \left(\frac{rs}{p_1}\right)^{n_1}\left(\frac{rs}{p_2}\right)^{n_2}\cdots\left(\frac{rs}{p_n}\right)^{n_m}\\ &= \left(\frac{r}{p_1}\right)^{n_1}\left(\frac{r}{p_2}\right)^{n_2}\cdots\left(\frac{r}{p_n}\right)^{n_m}\left(\frac{s}{p_1}\right)^{n_1}\left(\frac{s}{p_2}\right)^{n_2}\cdots\left(\frac{s}{p_n}\right)^{n_m}\\ &= \left(\frac{r}{n}\right)\left(\frac{s}{n}\right).\end{aligned}$$

3. With the help of Euler's Criterion we find $\left(\frac{r}{p}\right) \equiv r^{\frac{p-1}{2}}(\text{mod } p)$ for any integer r with $\gcd(r, p) = 1$, p being any odd prime. Then $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Consequently,

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)^{n_1}\left(\frac{-1}{p_2}\right)^{n_2}\cdots\left(\frac{-1}{p_n}\right)^{n_m}\\ &= (-1)^{\frac{n_1(p_1-1)}{2}+\frac{n_2(p_2-1)}{2}+\cdots+\frac{n_m(p_m-1)}{2}}.\end{aligned}$$

Now, n can be expressed as

$$\begin{aligned}n &= p_1^{n_1}p_2^{n_2}\cdots p_m^{n_m}\\ &= \{1+(p_1-1)\}^{n_1}\{1+(p_2-1)\}^{n_2}\cdots\{1+(p_m-1)\}^{n_m}.\end{aligned}$$

Here for each i, the term p_i-1 is even. Then we have $\{1+(p_i-1)\}^{n_i} \equiv 1+n_i(p_i-1)(\text{mod } 4)$. Also, $\{1+n_i(p_i-1)\}\{1+n_j(p_j-1)\} \equiv 1+n_i(p_i-1)+n_j(p_j-1)(\text{mod } 4)$ because $n_in_j(p_i-1)(p_j-1)$ is multiple of 4. Hence

$$n \equiv 1+n_1(p_1-1)+n_2(p_2-1)+\cdots+n_m(p_m-1)(\text{ mod } 4)$$

$$\frac{n-1}{2} \equiv \frac{n_1(p_1-1)}{2}+\frac{n_2(p_2-1)}{2}+\cdots+\frac{n_m(p_m-1)}{2}(\text{ mod } 2)$$

This shows that $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$.

4. In light of Theorem 9.2.8, for any odd prime p if $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{2}}$ holds then 2 becomes the quadratic residue provided $p \equiv \pm 1(\text{mod } 8)$. Thus, we find

$$\begin{aligned}\left(\frac{2}{n}\right) &= \left(\frac{2}{p_1}\right)^{n_1}\left(\frac{2}{p_2}\right)^{n_2}\cdots\left(\frac{2}{p_m}\right)^{n_m}\\ &= (-1)^{\frac{n_1(p_1^2-1)}{8}+\frac{n_2(p_2^2-1)}{8}+\cdots+\frac{n_m(p_m^2-1)}{8}}.\end{aligned}$$

Again, n can be expressed as $n^2 = \{1+(p_1^2-1)\}^{n_1}\{1+(p_2^2-1)\}^{n_2}\cdots\{1+(p_m^2-1)\}^{n_m}$. Since $p_i \equiv \pm 1(\text{mod } 8)$ then $p_i^2 \equiv 1(\text{mod } 8)$ or $p_i^2-1 \equiv 0(\text{mod } 8)$. Thus $\{1+(p_i^2-1)\}^{n_i} \equiv 1+n_i(p_i^2-1)(\text{mod } 64)$ and $\{1+n_i(p_i^2-1)\}\{1+n_j(p_j^2-1)\} \equiv 1+n_i(p_i^2-1)+n_j(p_j^2-1)(\text{mod } 64)$. Hence $n^2 \equiv 1+n_1(p_1^2-1)+n_2(p_2^2-1)+\cdots+n_m(p_m^2-1)(\text{mod } 64)$, which further implies $\frac{n^2-1}{8} \equiv \frac{n_1(p_1^2-1)}{8}+\frac{n_2(p_2^2-1)}{8}+\cdots+\frac{n_m(p_m^2-1)}{8}(\text{mod } 8)$. This yields $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$.

□

Now the following theorem highlights the fact that the reciprocity law agrees for both Jacobi symbol and the Legendre symbol.

Theorem 9.6.2. *Let m and n relatively prime odd positive integers. Then* $(\frac{m}{n})(\frac{n}{m}) = (-1)^{(\frac{m-1}{2})(\frac{n-1}{2})}$

Proof. Let $n = p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ and $m = q_1^{m_1}q_2^{m_2}\cdots q_s^{m_s}$ be prime factorizations of n and m respectively. Then,

$$\begin{aligned}\left(\frac{m}{n}\right) &= \prod_{i=1}^{r}\left(\frac{m}{p_i}\right)^{n_i}\\ &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)^{n_im_j} \quad \text{and}\\ \left(\frac{n}{m}\right) &= \prod_{j=1}^{s}\left(\frac{n}{q_j}\right)^{m_j}\\ &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)^{n_im_j}.\end{aligned}$$

Thus we get, $(\frac{m}{n})(\frac{n}{m}) = \prod_{i=1}^{r}\prod_{j=1}^{s}[(\frac{p_i}{q_j})(\frac{q_j}{p_i})]^{n_im_j}$. From the quadratic reciprocity law, we achieve $(\frac{p_i}{q_j})(\frac{q_j}{p_i}) = (-1)^{(\frac{p_i-1}{2})(\frac{q_j-1}{2})}$. Hence

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{(\frac{n_i(p_i-1)}{2})(\frac{m_j(q_j-1)}{2})}\\ &= (-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}(\frac{n_i(p_i-1)}{2})(\frac{m_j(q_j-1)}{2})}\\ &= (-1)^{\sum_{i=1}^{r}(\frac{n_i(p_i-1)}{2})\sum_{j=1}^{s}(\frac{m_j(q_j-1)}{2})}\\ &= (-1)^{(\frac{n-1}{2})(\frac{m-1}{2})}.\end{aligned}$$

This completes the proof. □

Our future effort is develop an elegant algorithm for evaluating Jacobi symbol. Let m and n be two relatively prime positive integers with $m > n$. Assume $J_0 = m$ and $J_1 = n$. Applying division algorithm on J_0 and J_1 we have, $J_0 = J_1 \cdot q_1 + 2^{t_1}J_2$ where q_1 is quotient and $2^{t_1}J_2$ is the remainder. Here, $2^{t_1}J_2$ is constructed in such a way that J_2 is an odd positive integer less than J_1; and t_1 be a non negative integer. Now the repeated use of division algorithm gives,

$$\begin{aligned}J_1 &= J_2 \cdot q_2 + 2^{t_2}J_3\\ J_2 &= J_3 \cdot q_3 + 2^{t_3}J_4\\ &= \vdots\\ J_{n-3} &= J_{n-2} \cdot q_{n-2} + 2^{t_{n-2}}J_{n-1}\\ J_{n-2} &= J_{n-1} \cdot q_{n-1} + 2^{t_{n-1}} \cdot 1,\end{aligned}$$

where each t_j is non-negative integer and J_i is an odd positive integer less than J_{i-1} for $i = 2, 3, \cdots n-1$. Here the sequence of equations get discontinued, where $J_k = 1$ for some positive integer k as $\gcd(m, n) = 1$.

To illustrate the algorithm, let us take $m = J_0 = 225$ and $n = J_1 = 29$. Then,

$$\begin{aligned} 225 &= 29 \cdot 7 + 2^1 \cdot 11 \\ 29 &= 11 \cdot 2 + 2^0 \cdot 7 \\ 11 &= 7 \cdot 1 + 2^2 \cdot 1 \end{aligned}$$

Formatting all our discussions in the following theorem, which demonstrates, how this algorithm evaluates Jacobi symbols.

Theorem 9.6.3. *Let m and n be positive integers with $m > n$. Then*

$$(\frac{m}{n}) = (-1)^{\frac{t_1(J_1^2-1)}{8} + \frac{t_2(J_2^2-1)}{8} + \cdots + \frac{t_{n-1}(J_{n-1}^2-1)}{8} + (\frac{J_1-1}{2})(\frac{J_2-1}{2}) + \cdots + (\frac{J_{n-2}-1}{2})(\frac{J_{n-1}-1}{2})},$$

where J_i and t_i are the integers for $i = 1, 2, \cdots n-1$ as described above.

Proof. By virtue of Theorem 9.6.1, we see that

$$\left(\frac{m}{n}\right) = \left(\frac{J_0}{J_1}\right) = \left(\frac{2^{t_1} J_2}{J_1}\right) = \left(\frac{2}{J_1}\right)^{t_1} \left(\frac{J_2}{J_1}\right) = (-1)^{\frac{t_1(J_1^2-1)}{8}} \left(\frac{J_2}{J_1}\right).$$

Again in the light of Theorem 9.6.2, we see that

$$(\frac{J_2}{J_1}) = (-1)^{\frac{J_1-1}{2}\frac{J_2-1}{2}} (\frac{J_1}{J_2}).$$

Combining them, gives

$$(\frac{m}{n}) = (-1)^{\frac{J_1-1}{2}\frac{J_2-1}{2} + \frac{t_1(J_1^2-1)}{8}} (\frac{J_1}{J_2}).$$

Continuing with these steps we get,

$$(\frac{J_{i-1}}{J_i}) = (-1)^{\frac{J_i-1}{2}\frac{J_{i+1}-1}{2} + \frac{t_i(J_i^2-1)}{8}} (\frac{J_i}{J_{i+1}}),$$

for $i = 2, 3, \cdots n-1$. Finally combining all those inequalities we obtain,

$$(\frac{m}{n}) = (-1)^{\frac{t_1(J_1^2-1)}{8} + \frac{t_2(J_2^2-1)}{8} + \cdots + \frac{t_{n-1}(J_{n-1}^2-1)}{8} + \left(\frac{J_1-1}{2}\right)\left(\frac{J_2-1}{2}\right) + \cdots + \left(\frac{J_{n-2}-1}{2}\right)\left(\frac{J_{n-1}-1}{2}\right)}.$$

□

Example 9.6.1. *Let $m = 225$ and $n = 29$. Then we get,*

$$\begin{aligned} \left(\frac{225}{29}\right) &= (-1)^{\frac{2(29^2-1)}{8} + \frac{0(11^2-1)}{8} + \frac{2(7^2-1)}{8} + (\frac{29-1}{2})(\frac{11-1}{2}) + (\frac{11-1}{2})(\frac{9-1}{2})}, \\ &= (-1)^{210+12+70+20} = (-1)^{312} = 1. \end{aligned}$$

Our previous discussion tells us about the solvability of quadratic congruence modulo odd prime p. Consider two composite numbers 441 and 1764, then factorize them as $441 = 3^2 \times 7^2$, $1764 = 2^2 \times 3^2 \times 7^2$. Thus an odd composite number can be represented as product of distinct odd primes and if the composite number is even, then in the factorization of it some powers of 2 occurs along with the product of distinct odd primes. If we consider an odd composite number $m = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ and an even composite number $n = 2^k p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$, then it is necessary to find solvability of quadratic congruences modulo 2^k and $p_i^{m_i}$ for each prime p_i and positive integers k, m_i. Solving the equations $x^2 \equiv r(\bmod m)$ and $x^2 \equiv r(\bmod n)$ is equivalent to solve the systems $x^2 \equiv r(\bmod 2^k)$, $x^2 \equiv r(\bmod p_1^{m_1}) \cdots x^2 \equiv r(\bmod p_n^{m_n})$. This motivates us to state and prove the following theorems, which deals with the solvability of quadratic congruences $x^2 \equiv r(\bmod p_i^{m_i})$ and $x^2 \equiv r(\bmod 2^k)$ for any odd prime p_i and $k > 0$.

Theorem 9.6.4. *If p is an odd prime and $\gcd(r, p) = 1$, then the congruence $x^2 \equiv r(\bmod p^n)$ $(n \geq 1)$ has a solution if and only if $(\frac{r}{p}) = 1$.*

Proof. For the 'if' part, let the congruence equation $x^2 \equiv r(\bmod p^n)$ has a solution. Then $x^2 \equiv r(\bmod p)$ is solvable. Hence $(\frac{r}{p}) = 1$.

For the 'only if' part, let $(\frac{r}{p})$ holds. We intend to use the principle of mathematical induction on n to prove the solvability of $x^2 \equiv r(\bmod p^n)$. The result is trivial for $n = 1$. Let us consider the statement prevails for $n = k$. Then $x^2 \equiv r(\bmod p^k)$ is solvable. For $n = k + 1$ its suffices to show that $x^2 \equiv r(\bmod p^{k+1})$ is solvable. As $x^2 \equiv r(\bmod p^k)$ is solvable, let $x = x_0$ be its solution. Then $x_0^2 = r + bp^k$ holds, for some integer b. To examine whether $x^2 \equiv r(\bmod p^k)$ is solvable, we need to find the solution of $2x_0 y \equiv -b(\bmod p)$. As $\gcd(2x_0, p) = 1$, therefore this linear congruence is solvable with its solution $y = y_0$.

Let us consider the integer $x_1 = x_0 + y_0 p^k$. Squaring we get,

$$\begin{aligned}(x_0 + y_0 p^k)^2 &= x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k} \\ &= r + (b + 2x_0 y_0) p^k + y_0^2 p^{2k}.\end{aligned}$$

Here $p \big| (b + 2x_0 y_0)$. Then applying congruence modulo p^{k+1} we get, $x^2 \equiv r(\bmod p^{k+1})$. Thus the statement is true for $n = k + 1$, so the induction step is complete. □

Let us illustrate Theorem 9.6.4 with an example, where we can find a solution of $x^2 \equiv 14(\bmod 5^2)$. To accomplish this, we see that $x^2 \equiv 14(\bmod 5)$ has a solution $x_0 = 7$ as $\left(\frac{4}{5}\right) = 1$. Now $7^2 = 49 = 14 + 7 \cdot 5$, where $b = 7$ and the linear equation $2 \times 7 \times y \equiv -7(\bmod 5)$ has a solution $y_0 = 2$. Thus

$x_1 = x_0 + y_0 p = 7 + 2 \times 5 = 17$. Let us examine, whether $x_1 = 17$ is the solution of $x^2 \equiv 14 (\bmod\ 5^2)$.

Now consider even composite number, where we can compute the case for modulo $2^k (k \geq 1)$. The following is the theorem based on that.

Theorem 9.6.5. *Let r be an odd integer. Then*

1. $x^2 \equiv r (\bmod\ 2)$ *always solvable.*
2. $x^2 \equiv r (\bmod\ 4)$ *has a solution if and only if* $r \equiv 1 (\bmod\ 4)$.
3. $x^2 \equiv r (\bmod\ 2^n)$, *for* $n \geq 3$ *has a solution if and only if* $r \equiv 1 (\bmod\ 8)$.

Proof. 1. Obvious.

2. Since the square of any odd integer congruent to 1 modulo 4, therefore r must be of the form $4k + 1$ to solve $x^2 \equiv r (\bmod\ 4)$. Thus the equation $x^2 \equiv r (\bmod\ 4)$ has a solution if and only if $r \equiv 1 (\bmod\ 4)$. In this case $x = 1$ and $x = 3$ are two solutions modulo 4.

3. Note that the square of any odd integer is congruent to 1 modulo 8. Then $x^2 \equiv r (\bmod\ 2^n)$ is solvable implies r is of the form $8m + 1$ for any integer m. This proves $r \equiv 1 (\bmod\ 8)$.

   Conversely, let $r \equiv 1 (\bmod\ 8)$ holds. With the help of mathematical induction, we will prove $x^2 \equiv r (\bmod\ 2^n)$ is solvable. Take $n = 3$. Then the congruence becomes $x^2 \equiv r (\bmod\ 8)$. Thus $x^2 \equiv 1 (\bmod\ 8)$ is certainly solvable. Here $x = 1, 3, 5, 7$ satisfies $x^2 \equiv 1 (\bmod\ 8)$. Thus the result is true for $n = 3$. Next, let us assume the result be true for $n = k (> 3)$. Then the congruence $x^2 \equiv r (\bmod\ 2^k)$ admits a solution x_0, which implies $\exists\ b \in \mathbb{Z}$ such that $x_0^2 = r + b \cdot 2^k$. As r is odd, so is the integer x_0. Thus $\gcd(x_0, 2) = 1$ leads to the fact that $x_0 y \equiv -b (\bmod\ 2)$ has a solution $y = y_0$. Choose an integer $x_1 = x_0 + y_0 2^{k-1}$. Then squaring we get,

$$\begin{aligned}(x_0 + y_0 2^{k-1})^2 &= x_0^2 + x_0 y_0 2^k + y_0^2 2^{2k-2} \\ &= r + (b + x_0 y_0) 2^k + y_0^2 2^{2k-2}\end{aligned}$$

   Here $2 | (x_0 y_0 + 2)$ yields $x^2 \equiv r (\bmod\ 2^{k+1})$. So the result becomes true for $n = k + 1$. Hence the converse part is established.

□

The final theorem of this section is the combined effect of the proof of last two theorems.

Theorem 9.6.6. *Let* $n(>1)$ *be a composite number with the prime factorization* $n = 2^k p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ *and* r *be any positive integer with* $\gcd(r, n) = 1$*. Then the congruence equation* $x^2 \equiv r (\bmod n)$ *is solvable if and only if*

1. $\left(\frac{r}{p_i}\right) = 1$ *for* $i = 1, 2, \cdots t$*;*

2. $r \equiv 1(\bmod 4)$*, if* $4|n$ *but* $8 \nmid n$*;* $r \equiv 1(\bmod 8)$*, if* $8|n$*.*

9.7 Worked out Exercises

Problem 9.7.1. *Evaluate the following Jacobi symbol* $(\frac{27}{101})$*.*

Solution 9.7.1. *Here we have,*

$$\begin{aligned}\left(\frac{27}{101}\right) =& \left(\frac{3}{101}\right)^3\\ =& \left(\frac{101}{3}\right)^3 [\textit{by Corollary 9.4.2 since } 101 \equiv 1(\bmod 4)]\\ =& \left(\frac{2}{3}\right)^3 = -1.\end{aligned}$$

Problem 9.7.2. *Let* a *and* b *are relatively prime integers such that* b *is odd and positive and* $a = (-1)^s 2^t q$ *where* q *is an odd integer. Prove that,*

$$\left(\frac{a}{b}\right) = (-1)^{(\frac{b-1}{2})s + (\frac{b^2-1}{8})t} \left(\frac{q}{b}\right).$$

Solution 9.7.2. *Note that* $\gcd(a, b) = 1$ *and* b *is an odd positive integer. As* $a = (-1)^s 2^t q$ *for any odd integer* q*, then it follows that*

$$\begin{aligned}\left(\frac{a}{b}\right) =& \left(\frac{(-1)^s 2^t q}{b}\right)\\ =& \left(\frac{-1}{b}\right)^s \left(\frac{2}{b}\right)^t \left(\frac{q}{b}\right)\\ =& (-1)^{(\frac{b-1}{2})s} (-1)^{(\frac{b^2-1}{8})t} \left(\frac{q}{b}\right)\\ =& (-1)^{(\frac{b-1}{2})s + (\frac{b^2-1}{8})t} \left(\frac{q}{b}\right).\end{aligned}$$

Problem 9.7.3. *For which positive integers* n *that are relatively prime to* 15 *does the Jacobi symbol* $(\frac{15}{n})$ *equal to* 1*.*

Solution 9.7.3. *An appeal to the reciprocity law of Jacobi symbol, for any integer* n *with* $\gcd(n, 15) = 1$ *it follows that*

$$\left(\frac{15}{n}\right) = \begin{cases} (\frac{n}{15}), & \textit{if } n \equiv 1(\mod 4) \\ -(\frac{n}{15}), & \textit{if } n \equiv 3(\mod 4). \end{cases}$$

Here $\left(\frac{n}{15}\right) = \left(\frac{n}{5}\right)\left(\frac{n}{3}\right)$ *and*

$$\left(\frac{n}{3}\right) = \begin{cases} 1, & \textit{if } n \equiv 1(\mod 3) \\ -1, & \textit{if } n \equiv 2(\mod 3) \end{cases}$$

$$\left(\frac{n}{5}\right) = \begin{cases} 1, & \textit{if } n \equiv 1 \textit{ or } 4(\mod 5) \\ -1, & \textit{if } n \equiv 2 \textit{ or } 3(\mod 5). \end{cases}$$

Combining we get,

$$\left(\frac{n}{15}\right) = \begin{cases} 1, & \textit{if } n \equiv 1, 2, 4, 8(\mod 15) \\ -1, & \textit{if } n \equiv 1, 7, 13, 14(\mod 15). \end{cases}$$

Applying Chinese Remainder Theorem, $(\frac{15}{n}) = 1$ *holds if and only if* $n \equiv 1, 7, 11, 17, 43, 53$ *or* $59(\mod 60)$ *(Verify!).*

Problem 9.7.4. *Let* n *be an odd square-free positive integer. Prove that there is an integer* a *such that* $\gcd(a, n) = 1$ *and* $(\frac{a}{n}) = -1$.

Solution 9.7.4. *As* n *is odd and square-free, it is of the form* $n = p_1 p_2 \cdots p_t$ *where each* p_i*'s are primes. Then* $(\frac{a}{n})$ *can be written as* $(\frac{a}{n}) = (\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{p_t})$. *Let us choose* b *as one of quadratic non residue among* $(\frac{p_1-1}{2})$ *numbers of quadratic non residues of* p_1. *This implies* $(\frac{b}{p_1}) = -1$. *As* $\gcd(a, n) = 1$ *and* $n = p_1 p_2 \cdots p_t$, *then applying Chinese Remainder Theorem we can assume* a *is a solution of the system* $x \equiv b(\mod p_1), x \equiv 1(\mod p_2), \cdots x \equiv 1(\mod p_t)$. *Then we have,* $(\frac{a}{p_1}) = (\frac{b}{p_1}) = -1, (\frac{a}{p_2}) = (\frac{1}{p_2}) = 1, \cdots (\frac{a}{p_t}) = (\frac{1}{p_t}) = 1$. *This proves that* $(\frac{a}{n}) = (\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{p_t}) = -1$.

Problem 9.7.5. *Using the Generalized Quadratic Reciprocity Law, determine whether the congruence* $x^2 \equiv 231(\mod 1105)$ *is solvable.*

Solution 9.7.5. *First note that* $231 = 3 \cdot 7 \cdot 11$ *and* $1105 = 5 \cdot 13 \cdot 17$ *with* $\gcd(231, 1105) = 1$. *For this we need to show either* $(\frac{231}{1105}) = 1$ *or* $(\frac{231}{1105}) = -1$.

Now $(\frac{231}{1105})(\frac{1105}{231}) = (-1)^{(\frac{231-1}{2})(\frac{1105-1}{2})} = 1$. *Thus we have,*

$$\begin{aligned}\left(\frac{231}{1105}\right) =& \left(\frac{1105}{231}\right) = \left(\frac{181}{231}\right)\\ =& \left(\frac{181}{3}\right)\left(\frac{181}{7}\right)\left(\frac{181}{11}\right)\\ =& \left(\frac{1}{3}\right)\left(\frac{6}{7}\right)\left(\frac{5}{11}\right)\\ =& \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{11}{5}\right) = -1\end{aligned}$$

So $x^2 \equiv 231 (\bmod 1105)$ *is not solvable.*

Problem 9.7.6. *Let us consider a positive integer* r *such that* r *is not a perfect square and satisfies* $r \equiv 0(\bmod 4)$ *or* $r \equiv 1(\bmod 4)$. *Now for this* r *we define Kronecker symbol as follows,*

$$\left(\frac{r}{2}\right) = \begin{cases} 1, & \textit{if } r \equiv 1(\bmod 8)\\ -1, & \textit{if } r \equiv 5(\bmod 8). \end{cases}$$

Now for this r *prove that,* $(\frac{r}{2}) = (\frac{2}{|r|})$ *if* $2 \nmid r$, *where the symbol of the right hand side is a Jacobi symbol.*

Solution 9.7.6. *If* $r > 0$, *then clearly* $(\frac{2}{|r|}) = (\frac{2}{r})$ *and by Theorem 9.6.1 we have* $(\frac{2}{r}) = (-1)^{\frac{r^2-1}{8}}$. *Also if* $r < 0$, *then* $(\frac{2}{|r|}) = (\frac{2}{-r}) = (-1)^{\frac{(-r)^2-1}{8}} = (-1)^{\frac{r^2-1}{8}}$. *But here* $2 \nmid r$ *means* r *is odd and* $r \equiv 1(\bmod 4)$ *together gives* $r \equiv 1(\bmod 8)$ *and* $r \equiv 5(\bmod 8)$. *Now for* $r \equiv 1(\bmod 8)$ *and* $r \equiv 5(\bmod 8)$ *we see that* $(-1)^{\frac{r^2-1}{8}} = 1$ *and* $(-1)^{\frac{r^2-1}{8}} = -1$ *holds respectively. Together these two assertions imply* $(\frac{r}{2}) = (\frac{2}{|r|})$.

Problem 9.7.7. *Find the solution of* $x^2 + 5x + 6 \equiv 0(\bmod 5^3)$.

Solution 9.7.7. *Here* $x^2 + 5x + 6 \equiv 0(\bmod 5^3) \Rightarrow (x+3)(x+2) \equiv 0(\bmod 5^3)$. *Therefore* $x \equiv -3, -2 \equiv 122, 123(\bmod 5^3)$.

Problem 9.7.8. *Solve the following quadratic congruence:* $x^2 \equiv 2(\bmod 7^3)$.

Solution 9.7.8. *To solve this equation, we start with the congruence equation* $x^2 \equiv 2(\bmod 7)$. *The solution of this equation is* $x_0 = 3$. *Now* $x_0^2 = 3^2 = 2 + b \cdot 7 \Rightarrow b = 1$. *Now the linear equation* $2 \cdot 3 \cdot y \equiv -1(\bmod 7)$ *has the solution* $y_0 = 1$. *So* $x_1 = x_0 + y_0 \times 7 = 10$ *is the solution of* $x^2 \equiv 2(\bmod 7^2)$.

Further, $x^2 \equiv 2(\bmod 7^2)$ *has the solution* $x_0 = 10$. *Now* $x_0^2 = 10^2 = 2 + b \cdot 49 \Rightarrow b = 2$. *The linear equation* $2 \cdot 10 \cdot y \equiv -2(\bmod 7)$ *has the solution* $y_0 = 2$. *So* $x_1 = x_0 + y_0 \times 49 = 108$ *is the solution of* $x^2 \equiv 2(\bmod 7^3)$. *Thus the final solutions are* $x \equiv 108, -108 \equiv 108, 235(\bmod 7^3)$.

Problem 9.7.9. *First determine the values of a for which the congruence is solvable and then find the solution of that: $x^2 \equiv a (\bmod 2^5)$.*

Solution 9.7.9. *Note that $x^2 \equiv a (\bmod 2^5)$ is solvable, if $a \equiv 1 (\bmod 8)$ (Why?). Therefore $a = 1, 9, 17$ or 25 as $2^5 = 32$.*

For $a = 1$: $x \equiv \pm 1,\ \pm 1 + 2^4 \equiv 1, 15, 17, 31 (\bmod 2^5)$.

For $a = 9$: $x \equiv \pm 3,\ \pm 3 + 2^4 \equiv 3, 13, 19, 29 (\bmod 2^5)$.

For $a = 17$: $x^2 \equiv 17{+}32 (\bmod 2^5)\ \therefore x \equiv \pm 7,\ \pm 7{+}2^4 \equiv 7, 9, 23, 25 (\bmod 2^5)$.

For $a = 25$: $x \equiv \pm 5,\ \pm 5 + 2^4 \equiv 5, 11, 21, 27 (\bmod 2^5)$.

Problem 9.7.10. *Prove that if the congruence $x^2 \equiv a (\bmod 2^n)$, where a is odd and $n \geq 3$, has a solution, then it has exactly four incongruent solutions.*

Solution 9.7.10. *From Theorem 8.6.3, it follows that 2^n has no primitive root for $n \geq 3$. Thus $x^2 \equiv a (\bmod 2^n)$ has a solution.*

Since a is odd and x_0 is a solution, then x_0 must be odd. Also $-x_0$ is a solution. Let x_1 be any other solution. Then $x_1^2 \equiv a (\bmod 2^n)$ implies $x_1^2 \equiv x_0^2 (\bmod 2^n)$ for $n \geq 3$. Therefore $(x_1{+}x_0)(x_1{-}x_0) \equiv 0 (\bmod 2^n) \Rightarrow (\frac{x_1+x_0}{2})(\frac{x_1-x_0}{2}) \equiv 0 (\bmod 2^{n-2})$, $n \geq 3$. But here $\frac{x_1+x_0}{2} + \frac{x_1-x_0}{2} = x_1$ is odd, so any one of them is even.

If $\frac{x_1-x_0}{2}$ is even and $\frac{x_1+x_0}{2}$ is odd, then $(x_1 - x_0)(\frac{x_1+x_0}{2}) \equiv 0 (\bmod 2^{n-1}) \Rightarrow x_1 \equiv x_0 (\bmod 2^{n-1})$.

On the other hand if $\frac{x_1-x_0}{2}$ is odd and $\frac{x_1+x_0}{2}$ is even, then $(x_1{+}x_0)(\frac{x_1-x_0}{2}) \equiv 0 (\bmod 2^{n-1}) \Rightarrow x_1 \equiv -x_0 (\bmod 2^{n-1})$. Thus together we have $x_1 = \pm x_0 + k2^{n-1}$.

If k is odd then for $k = 2r+1$ we have, $x_1 = \pm x_0 + 2^{n-1} + r2^n \equiv \pm x_0 + 2^{n-1} (\bmod 2^n)$.

If k is even then for $k = 2r$ we have, $x_1 = \pm x_0 + r2^n \equiv \pm x_0 (\bmod 2^n)$.

Therefore the only incongruent solutions are $\pm x_0,\ \pm x_0 + 2^{n-1}$.

9.8 Exercises:

1. Find the solutions of the following quadratic congruences:
   (a) $x^2 + 5x + 1 \equiv 0 (\bmod 7)$
   (b) $x^2 + 7x + 10 \equiv 0 (\bmod 11)$
   (c) $5x^2 + 6x + 1 \equiv 0 (\bmod 23)$.
2. Given that a is a quadratic residue of the odd prime p, prove that a is not a primitive root of p.

3. Let p be an odd prime and $\gcd(a,p) = 1$. Establish that the quadratic congruence $ax^2 + bx + c \equiv 0(\text{mod } p)$ is solvable if and only if $b^2 - 4ac$ is either zero or a quadratic residue of p.

4. Find all the quadratic residues of 19, where 2 is a primitive root of 19.

5. Evaluate the following Legendre symbols:

   (a) $(\frac{19}{23})$ (b)$(\frac{-23}{59})$ (c)$(\frac{18}{43})$ (d)$(\frac{461}{773})$ (e)$(\frac{-219}{383})$ (f)$(\frac{111}{991})$.

6. Use Gauss's lemma to compute each of the Legendre symbols below :

   (a) $(\frac{8}{11})$ (b)$(\frac{5}{19})$ (c)$(\frac{11}{23})$.

7. Let a and b be integers not divisible by prime p. Show that there is either one or three quadratic residues among the integers a, b and ab.

8. Given a prime p, show that, for some choice of $n > 0$, p divides

$$(n^2 - 2)(n^2 - 3)(n^2 - 6)$$

9. If the prime $p > 5$, show that p divides the sum of the squares of its quadratic nonresidues.

10. Given that p and $q = 4p+1$ are both primes, then prove that any quadratic nonresidue of q is either a primitive root of q or has order 4 modulo q.

11. Determine whether the given quadratic congruence is solvable $2x^2 + 5x - 9 \equiv 0(\text{mod } 101)$.

12. Find a congruence describing all primes for which 7 is a quadratic residue.

13. Prove that there are infinitely many primes of the form $5k - 1$.

14. Verify that the prime divisors p of the integer $2n(n+1)+1$ are of the form $p \equiv 1(\text{mod } 4)$.

15. Solve the quadratic congruence $x^2 \equiv 11(\text{mod } 35)$.

16. Evaluate the following Jacobi symbols:

    (a) $(\frac{1009}{2307})$ (b)$(\frac{2663}{3299})$ (c)$(\frac{10001}{20003})$.

17. For which positive integers n that are relatively prime to 30 does the Jacobi symbol $(\frac{30}{n})$ equal to 1.

18. Evaluate the following Kronecker symbol:

    (a) $(\frac{5}{12})$ (b)$(\frac{101}{200})$.

19. Show that if n_1 and n_2 be positive integers with $\gcd(a, n_1n_2) = 1$, then $(\frac{a}{n_1n_2}) = (\frac{a}{n_1})(\frac{a}{n_2})$.

20. Show that if n_1 and n_2 are positive integers relatively prime to a and $n_1 \equiv n_2(\text{mod } |a|)$, then $(\frac{a}{n_1}) = (\frac{a}{n_2})$.

21. Solve the congruence $x^2 \equiv 31(\text{mod } 11^4)$.

22. Solve each of the following quadratic congruences:

    (a) $x^2 \equiv 7(\text{mod } 3^3)$;

    (b) $x^2 \equiv 14(\text{mod } 5^3)$.

23. Solve the congruence $x^2 \equiv 9(\text{mod } 2^3 \cdot 3 \cdot 5^2)$.

24. Show that 7 and 18 are the only incongruent solutions of $x^2 \equiv -1(\text{mod } 5^2)$.

25. Solve the congruence $2x^2 + 1 \equiv 0(\text{mod } 11^2)$.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

10

Integers of Special Forms

> *"An equation means nothing to me unless it expresses a thought of God."*
>
> – Srinivasa Ramanujan

10.1 Introduction

Over the centuries, integers with certain properties were studied extensively by several mathematicians. Present chapter portrayed few integers viz Perfect number, Mersenne Primes and Fermat number, where various theorems together with few properties are proved. We begin with the notion of perfect number.

10.2 Perfect Numbers

In ancient times, Greek Mathematicians have found some interesting integers which can be written as sum of their divisors. For example $6 = 1 + 2 + 3$ where $1, 2, 3$ are divisors of 6. They have named those type of integers as perfect integers or perfect numbers. Thus the definition of perfect number are as follows:

Definition 10.2.1. *If n is a positive integer with $\sigma(n) = 2n$, then n is said to be a perfect number.*

For example we have

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28.$$
$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6.$$

Here $6, 28$ are perfect numbers.

Also, the Greek Mathematicians discovered the method of finding an even perfect number. Here the perfect number $6, 28$ can be written as $6 = 2 \cdot 3 = 2^{2-1}(2^2 - 1), 28 = 2^{3-1}(2^3 - 1) = 4 \cdot 7$ respectively. Thus the numbers are in the multiplication of even and prime numbers. Euclid first tried to find the form of a perfect number. After 2000 years Euler gave us a concrete proof about the form of a perfect number. Now the following theorem deals with the form of a perfect number.

Theorem 10.2.1. *For any positive integer* n *is an even perfect number if and only if it is of the form* $n = 2^{k-1}(2^k - 1)(k > 1), 2^k - 1$ *being prime.*

Proof. Let $p = 2^k - 1$. Then $n = 2^{k-1}p$. Since, $k > 1$ then 2^{k-1} is not a prime and $\gcd(2^{k-1}, p) = 1$. From the theorem, the sum of divisor function σ is multiplicative. Then

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p)\\ &= \sigma(2^{k-1})\sigma(p)\\ &= \frac{2^{(k+1)-1} - 1}{2 - 1} \times (p + 1) \text{ [from Theorem 6.2.2]}\\ &= (2^k - 1)(p + 1)\\ &= 2^k(2^k - 1) = 2n,\end{aligned}$$

which shows n is a perfect number.

Conversely, let n be an even perfect number. Then for some positive integer s and positive odd integer t, $n = 2^s t$. Since, $\gcd(2^s, t) = 1$, from Theorem 6.2.3 applying multiplicative property of σ we have $\sigma(n) = \sigma(2^s t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t)$. Since, n is perfect, thus we have

$$\sigma(n) = 2n = 2^{s+1}t.$$

Combining we get, $2^{s+1}t = (2^{s+1} - 1)\sigma(t)$. As $\gcd(2^{s+1}, 2^{s+1} - 1) = 1$, then $2^{s+1}|\sigma(t)$. Thus there exists an integer q satisfying $\sigma(t) = 2^{s+1} \cdot q$. Thus we have,

$$(2^{s+1} - 1) \cdot 2^{s+1} \cdot q = 2^{s+1} \cdot t.$$

$$\text{Therefore } (2^{s+1} - 1)q = t,$$

which shows $q|t$ and $q \neq t$, for if $q = t$ then $2^{s+1} - 1 = 1 \Rightarrow s = 0$, which is not possible. Now $t + q = (2^{s+1} - 1)q + q = 2^{s+1} \cdot q = \sigma(t)$. Next our claim is $q = 1$ otherwise t will be a composite number. If $q \neq 1$ then the divisors of t are $1, q$ and t implies $\sigma(t) \geq 1 + q + t$, contradicts the fact $\sigma(t) = q + t$. Hence $q = 1$ and $t = 2^{s+1} - 1, \sigma(t) = t + 1$ which together shows t is prime. Thus, $n = 2^s(2^{s+1} - 1)$, where $2^{s+1} - 1$ is prime. Taking $s = k - 1$, we have $s > 0 \Rightarrow k > 1$ and $n = 2(k - 1)(2^k - 1)$. Hence the proof. ☐

From the above theorem, it is clear that if our tasks is to find even perfect number then we only need to check the primes which is of the form $2^n - 1$. In search of that we first show that the exponent n must be prime. Our next theorem deals with it.

Theorem 10.2.2. *If n is a positive integer and $2^n - 1$ is prime then n must be prime.*

Proof. Let us assume, n be not prime. Then n is of the form $n = rs,\ 1 < r, s < n$. Then

$$2^n - 1 = (2^r)^s - 1.$$

$$\text{Therefore } 2^n - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \ldots + 1).$$

Here in the right hand side, both the factors are greater than 1 which shows $2^n - 1$ is composite if n is so. Thus if $2^n - 1$ is prime then n must be prime. ☐

In particular, if we take $n = 2, 3, 5$ then $2^n - 1 = 3, 7, 31$ are all primes, which shows that $2(2^2 - 1) = 6, 2^2(2^3 - 1) = 28, 2^4(2^5 - 1) = 496$ are all perfect numbers. It is to be noted that all the even perfect number ends with 6m or 8. Since, the prime number set is countably infinite, therefore the numbers of the form $2^p - 1$ is also infinite, for some prime p. As a consequence, we conclude that the perfect number set is countably infinite. Now the question arises: Does all the even perfect number ends with 6 or 8? The following theorem deals with this fact:

Theorem 10.2.3. *Every even perfect number ends with either 6 or 8 i.e.either $n \equiv 6 (\text{mod } 10)$ or $n \equiv 8 (\text{mod } 10)$.*

Proof. Let n be an even perfect number. Then n is of the form $n = 2^{k-1}(2^k - 1)(k > 1), where 2^{k-1}$ is a prime number. Now since 2^{k-1} is prime, k is also so(Why!). The case is trivial if we choose $k = 2$, then $n = 6$. Now our claim is to prove the statement for $k > 2$. Since, k is prime and greater than 2, it must be odd. So k must be of the form $4t + 1$ or $4t + 3$ for any positive integer t. Now, in the rest part of the theorem our claim is to show

1. the last digit 6 corresponds to $4t + 1$ or

2. the last digit 8 corresponds to $4t+3$.

To fulfill the above claims, further we need to prove $16^m \equiv 6 (\bmod 10)$.

Applying principle of mathematical induction we see that the case is trivial for $m=1$. Let for $m=r$, $16^r \equiv 6 (\bmod 10)$, holds true. Now for $m=r+1$, we have

$$16^{r+1} = 16^r \cdot 16 \equiv 6 \cdot 16 (\mod 10).$$

$$\text{Therefore } 16^{r+1} \equiv 36 (\mod 10) \equiv 6 (\mod 10).$$

Next to fulfill claim(1), let us take $k = 4t+1$. Then,

$$n = 2^{4t+1-1}(2^{4t+1}-1) = 2^{8t+1} - 2^{4t} = 2 \cdot 16^{2t} - 16t.$$

Hence $n \equiv 2 \cdot 6 - 6 (\bmod 10) \equiv 6 (\bmod 10)$(How!).

For claim(2), taking $k = 4t+3$ we obtain

$$n = 2^{4t+2}(2^{4t+3}-1) = 2^{8t+5} - 2^{4t+2} = 2 \cdot 16^{2t+1} - 4 \cdot 16^t.$$

Hence $n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 (\bmod 10) \Rightarrow n = 8 (\bmod 10)$. Consequently, every even perfect number has a last digit ends with 6 or 8.

□

Let us continue our discussion on the last digit of an even perfect number more deeply with some examples. In our foregoing examples instead of taking $k=3$ which gives $n=28$, if we take $k=7$, we have $n = 2^6(2^7-1) = 8128$. Here the last two digits are $2, 8$. This is not a coincidence, in fact in our next corollary we have shown how the last two digits always become 28.

Corollary 10.2.1. *An even perfect number n ends with either* 6 *or* 28.

Proof. The case of last digit 6 follows form the above theorem. For the remaining part, let us take $n = 2^{k-1}(2^k-1)(k>1), 2^{k-1}$ being prime. Since n is an even perfect number and $k = 4t+3$ for a positive integer t, we have

$$2^{k-1} = 2^{4t+2} = 16^t \cdot 4 \equiv 6 \cdot 4 (\mod 10) \equiv 4 (\mod 10).$$

As $k > 2$ then $4 | 2^{k-1}$ and the number formed by last two digits of 2^{k-1} is divisible by 4. Then under congruent modulo 100, the possibilities are $2^{k-1} \equiv 4, 24, 44, 64$ or $84 (\bmod 100)$. Since the last digit is 4, therefore $2^{k-1} \equiv 4 (\bmod 10)$. Now, let us take $2^{k-1} \equiv 4 (\bmod 100)$ then $2 \cdot 2^{k-1} \equiv 2 \cdot 4 - 10 (\bmod 100) \equiv 7 (\bmod 100)$ and so on. Then we have,

$$2^k - 1 = 2 \cdot 2^{k-1} - 1 \equiv 7, 47, 87, 27 \text{ or } 67 (\mod 100)$$

Thus multiplying, we have

$$n = 2^{k-1}(2^k - 1) \equiv (4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27) \text{ or } 84 \cdot 67 (\mod 100),$$
$$\Rightarrow n \equiv 28 (\mod 100) (\text{Verify!}).$$

□

The above discussions help us to recognize the form of an even perfect number. Here we conclude our discussions with some properties to elaborate even perfect number related to triangular number, a number which can be arranged in triangular form.

For instance, let us consider $3 = 1+2; 6 = 1+2+3; 10 = 1+2+3+4; 15 = 1+2+3+4+5; 21 = 1+2+3+4+5+6; 28 = 1+2+3+4+5+6+7; 36 = 1+2+3+4+5+6+7+8; 45 = 1+2+3+4+5+6+7+8+9, \ldots$, which can be arranged in triangular form as shown in the diagram below.

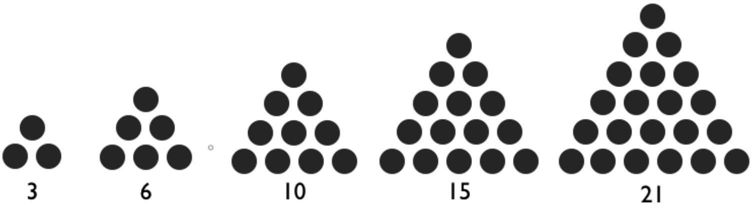


Figure 10.1: Triangular Diagram

Our next result focusses on the relation between them.

Proposition 10.2.1. *If N is an even perfect number then N is triangular.*

Proof. Let us choose a triangular number n. Then n can be written as $n = 1 + 2 + 3 + \cdots + r = \frac{1}{2}r(r-1)$ for some integer r. Now, since N is a perfect number N is of the form,

$$N = 2^{k-1}(2^k - 1) = \frac{1}{2}(2^k)(2^{k-1}),$$

which shows N is of the triangular form. This proves N is triangular.

□

We can also write perfect number as a sum of cubes by our next proposition.

Proposition 10.2.2. *If N is an even perfect number then $N = 1^3 + 2^3 + \ldots + (2^{\frac{n+1}{2}} - 1)^3$, $n > 1$.*

Proof. Let us consider $m = 2^{\frac{n-1}{2}}$. Then,

$$\begin{aligned} 1^3 + 2^3 + \ldots + (2m-1)^3 &= (1^3 + 2^3 + \ldots + (2m)^3) - (2^3 + 4^3 + \ldots + (2m)^3) \\ &= \frac{(2m)^2(2m+1)^2}{4} - 2^3 \times \frac{(m)^2(m+1)^2}{4} \\ &= m^2(2m^2-1). \end{aligned}$$

On substituting the value of m, we obtain

$$1^3 + 3^3 + \ldots + (2^{\frac{n+1}{2}} - 1)^3 = 2^{n-1}(2^n - 1) = N(Why!).$$

$\square$

10.3 Worked out Exercises

Problem 10.3.1. *Show that the integer $n = 2^{10}(2^{11}-1)$ is not a perfect number.*

Solution 10.3.1. *Note that $n = 2^{10}(2^{11}-1)$. To show n is a perfect number, it's suffices to show that $\sigma(n) = 2n$. Since $\gcd(2^{10}, 2^{11}-1) = 1$, therefore $\sigma(n) = \sigma(2^{10})\sigma(2^{11}-1)$ as σ is multiplicative.*

Furthermore, $2^{11}-1$ has a prime factorization given by $2^{11}-1 = 23 \cdot 89$. For any prime p, $\sigma(p) = p+1$ holds. Then $\sigma(2^{11}-1) = \sigma(23)\sigma(89) = 24 \times 90$ yields,

$$\begin{aligned} \sigma(n) &= 2^{11} \times (1 - \frac{1}{2}) \times 24 \times 90 \\ &= 2^{10} \times 24 \times 90 \\ &\neq 2^{11} \times (2^{11} - 1) \\ &\neq 2n. \end{aligned}$$

Therefore n is not a perfect number.

Problem 10.3.2. *Verify that no power of a prime can be a perfect number.*

Solution 10.3.2. *Let p be a prime and n be any positive integer. We claim that $\sigma(p^n) \neq 2p^n$. But $\sigma(p^n) = 1 + p + p^2 + \cdots + p^n = \frac{p^{n+1}-1}{p-1}$. Consider $p = 2$. Then $\sigma(2^n) = 2^{n+1} - 1 \neq 2^{n+1}$. Let the assertion be true for $p > 2$. Then $p^{n+1} - 1 = 2p^n(p-1)$ holds. It follows that,*

$$\begin{aligned} & p^{n+1} - 1 = 2p^{n+1} - 2p^n \\ \Rightarrow\ & p^{n+1} - 2p^n + 1 = 0 \\ \Rightarrow\ & p^n(p-2) = -1. \end{aligned}$$

This leads to a contradiction, as p^n *and* $p-2$ *are greater than or equal to* 1. *This proves* p^n *is not a perfect number.*

Problem 10.3.3. *For any perfect number* n *show that* $\sum_{d|n}(\frac{1}{d}) = 2$.

Solution 10.3.3. *As* n *is a perfect number, so* $\sigma(n) = 2n$. *Further we have* $\sigma(n) = \sum_{d|n} d$. *Combining the pieces, we get* $\sum_{d|n} d = 2n$. *Multiplying both sides by* $\frac{1}{n}$ *gives,*

$$\frac{1}{n}\sigma(n) = \frac{1}{n}\sum_{d|n} d = 2.$$

Referring to Problem 6.3.4, we have $\sum_{d|n}(\frac{1}{d}) = 2$.

Problem 10.3.4. *Prove that no divisor of a perfect number can be perfect.*

Solution 10.3.4. *Let* m *be a proper divisor of a perfect number* n. *As* n *is perfect, so the last problem generates* $\sum_{d|n}\frac{1}{d} = 2$. *Thus* $\sum_{d|m}\frac{1}{d} < \sum_{d|n}\frac{1}{d} = 2$. *This proves* m *is not perfect.*

Problem 10.3.5. *Find the last two digits of the perfect number* $n = 2^{19936}(2^{19937} - 1)$.

Solution 10.3.5. *Since* $\gcd(2,25) = 1$, *therefore using the Euler's Theorem we get* $2^{\phi(25)} \equiv 1(\mod 25)$ *i.e.* $2^{20} \equiv 1(\mod 25)$. *This implies* $2^{19334} \equiv 2^{14}(\mod 25)$. *Further* $2^{14} \equiv 9(\mod 25)$. *Stitching the facts, we get* $2^{19336} \equiv 4\cdot 9(\mod 100)$. *Therefore* $2^{19337} \equiv 72(\mod 100)$, *which shows that,*

$$\begin{aligned}2^{19936}(2^{19937} - 1) &\equiv 36 \times 71(\mod 100)\\ &\equiv 56(\mod 100).\end{aligned}$$

Therefore the last two digits of the perfect number is 56.

Problem 10.3.6. *Prove that there are the only two* 3*-perfect number of the form* $n = 2^k\cdot 3\cdot p$ *for any odd prime* p.

Solution 10.3.6. *If for any positive integer* n, $\sigma(n) = kn$ *for* $k \geq 3$ *holds then* n *is called* k*-perfect number. Thus for* 3*-perfect number we have* $\sigma(n) = 3n$. *We claim that, for any odd prime* p *the integers* 120 *and* 672 *are the only* 3*-perfect numbers of the form* $n = 2^k\cdot 3\cdot p$.

Assume $p = 3$. *Then* $n = 2^k\cdot 3^2$. *Thus* $\sigma(n) = \sigma(2^k)\sigma(3^2) = 13(2^{k+1} - 1)$. *This yields* $\sigma(n) = 3n$, *which is not possible as* $13 \nmid 3n$.

Now consider $p > 3$. *Then*

$$\begin{aligned}3n &= \sigma(n)\\ &= \sigma(2^k)\sigma(3)\sigma(p)\\ &= (2^{k+1}-1)\times 4\times(p+1).\end{aligned}$$

If $k = 0$, *then* $\sigma(n) = 4\times(p+1) \neq 9p$ *and if* $k = 1$ *then* $\sigma(n) = 12\times(p+1) \neq 6p$. *This shows that* k *is always greater than* 1. *Taking advantage of this form of* n *and dividing by* 4 *we find,*

$$2^{k-2}\cdot 3^2\cdot p = (2^{k+1}-1)(p+1). \tag{10.3.1}$$

But $\gcd(p, p+1) = \gcd(2^{k-2}, 2^{k+1}-1) = 1$, *which implies* $p|2^{k+1}-1$ *and* $2^{k-2}|p+1$. *Thus from the (10.3.1) we obtain,* $2^{k-2}\cdot 3^2\cdot p = p\cdot t_1\cdot 2^{k-2}\cdot t_2$ *for some integer* t_1, t_2. *This gives* $t_1t_2 = 9$. *So three cases may arise:*

1. *If* $t_1 = 1, t_2 = 9$ *holds, then we have* $p+1 = 9\cdot 2^{k-2}$ *and* $2^{k+1}-1 = p$. *The last two equations together gives* $9\cdot 2^{k+2} = 2^{k+1}$, *which is not possible.*
2. *If* $t_1 = 9, t_2 = 1$ *holds, then* $p+1 = 2^{k-2}$ *and* $2^{k+1}-1 = 9\cdot p$ *implies* $9\cdot 2^{k-2} - 9 = 2^{k+1}-1$. *On solving we get* $p = 7$, $k = 5$.
3. *If* $t_1 = 3, t_2 = 3$ *holds. Then we have* $p+1 = 3\cdot 2^{k-2}$ *and* $2^{k+1}-1 = 3\cdot p$ *.Then solving we get* $p = 5$, $k = 3$.

Thus the possible values are $n = 2^5\times 3\times 7 = 672$ *and* $n = 2^3\times 5\times 3 = 120$.

Problem 10.3.7. *If* $n > 6$ *is an even perfect number, prove that* $n \equiv 4 (\bmod 6)$.

Solution 10.3.7. *Here* $n > 6$ *is even perfect number, so it is of the form* $2^{k-1}(2^k-1)$ *where* $k(>2)$ *and* 2^k-1 *are odd primes. Since* $\gcd(2,3) = 1$, *therefore by Fermat's theorem* $2^{k-2}(2^k-1) \equiv 2(2-1)(\bmod 3) \Rightarrow 2^{k-1}(2^k-1) \equiv 4(\bmod 6)$. *Hence* $n \equiv 4(\bmod 6)$.

Problem 10.3.8. *Let* n *be a positive integer. Define the sequence* $n_1, n_2, n_3, \cdots$ *recursively by* $n_1 = \sigma(n) - n$ *and* $n_{k+1} = \sigma(n_k) - n_k$ *for* $k = 1, 2, 3, \cdots$. *Prove that if* n *is perfect, then* $n = n_1 = n_2 = \cdots$.

Solution 10.3.8. *Let* $n = n_1$ *be perfect. Then* $n_2 = \sigma(n) - n = 2n - n = n = n_1$. *Continuing this way at* j*-th stage we get,*

$$n_j = \sigma(n_{j-1}) - n_{j-1} = \sigma(n) - n = n,\ \forall j \geq 1.$$

This proves that $n = n_1 = n_2 = \cdots$.

Problem 10.3.9. *For any even perfect number* $n = 2^{k-1}(2^k - 1)$*, prove that* $2^k | (\sigma(n^2) + 1)$*.*

Solution 10.3.9. *As* n *is perfect, so it is of the form* $n = 2^{k-1}(2^k - 1)$ *where* $2^k - 1$ *is prime. As* $\gcd(2^k - 1, 2^{k-1}) = 1$*, then*

$$\begin{aligned}\sigma(n^2) &= \sigma(2^{2k-2})\sigma((2^k - 1)^2)\\ &= (1 + 2 + \cdots + 2^{2k-2})(1 + 2^k - 1 + (2^k - 1)^2)\\ &= (2^{2k-1} - 1)(2^{2k} - 2^k + 1)\\ &= 2^{2k-1}(2^{2k} - 2^k + 1) - 2^{2k} + 2^k - 1.\end{aligned}$$

From this it is clear that $2^k \Big| (\sigma(n^2) + 1)$*.*

Problem 10.3.10. *A number* n *is said to be super perfect number if* $\sigma(\sigma(n)) = 2n$*. Now using this concept of superperfect number, show that if* $n = 2^k$ *with* $2^{k+1} - 1$ *a prime, then* n *becomes a super perfect number.*

Solution 10.3.10. *Here* $n = 2^k$*. Then* $\sigma(n) = \sigma(2^k) = 2^{k+1} - 1$*. As* $2^{k+1} - 1$ *is prime, so* $\sigma(\sigma(n)) = \sigma(2^{k+1} - 1) = 2^{k+1} = 2n$*. Thus* 2^k *is super perfect number.*

Problem 10.3.11. *Let* n *be a non perfect positive integer. Then* n *is called deficient if* $\sigma(n) < 2n$ *and is called abundant if* $\sigma(n) > 2n$*. Every non perfect positive integer is either deficient or abundant. If* n *does not satisfy both the conditions then it is called perfect number.*

Now using this fact prove that every prime power is deficient.

Solution 10.3.11. *Pick* $n = p^k$ *for some prime* p *and positive integer* k*. Then we have,* $\sigma(p^k) = \dfrac{p^{k+1} - 1}{p - 1}$*. As* $p \geq 2$*, then* $2p^k - 1 < p^{k+1}$ *is always true. It follows that* $p^{k+1} - 1 < 2(p^{k+1} - p^k) = 2p^k(p - 1)$*. Thus* $\dfrac{p^{k+1} - 1}{p - 1} < 2p^k = 2n$ *justifies* n *as deficient.*

10.4 Mersenne Primes

Our earlier discussions on pseudoprime[refer to chapter-5] based on Fermat's Little theorem, where for any composite integer n, $2^n - 1$ is a pseudoprime. Any number of the form $2^n - 1$ is known to be n-th Mersenne number, after French Mathematician Father Marin Mersenne. Now, the present section deals with seeking some prime numbers of that form. From previous section, we have seen that for any positive integer n, if $2^n - 1$ is prime then n must be prime. But in general the converse of the last statement is not true, which gives birth to the notion of Mersenne prime *i.e.* for any prime p, if the integer $2^p - 1$ is also prime then it is said to be Mersenne prime. Using the results on Mersenne Prime, we will discuss various methods of primality testing.

Mersenne primes are used in the Mersenne twister PRNG (pseudo-random number generator), these are used extensively in simulations, Montecarlo methods, etc. The CWC mode for block ciphers can uses M_{127} as a prime number because $x(\bmod 2^{127} - 1)$ is very easy to compute.

Definition 10.4.1. *If p is a prime and $M_p = 2^p - 1$ is also so, then M_p is called Mersenne prime.*

Example 10.4.1. *The Mersenne number $M_7 = 2^7 - 1$ is prime but the Mersenne number $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ is not so. Here M_7 is Mersenne prime but M_{11} is not.*

Here in the above example we have seen that M_7 is prime but M_{11} is composite. Thus the formula that $2^p - 1$ is prime for any prime p fails to be true in general. So the hope for constructing prime numbers using this formula goes in vain. Now our next discussions focusses on constructing various methods for determining whether this special types of Mersenne numbers are prime or not. In next theorem, we have presented one particular type of test based on that.

Theorem 10.4.1. *If p and $p' = 2p + 1$ are primes then p' does not divide both M_p and $M_p + 2$ together.*

Proof. Since p' is prime then by Fermat's Little Theorem we have, $2^{p'-1} \equiv 1(\bmod p')$

$$\begin{aligned}
&\therefore 2^{p'-1} - 1 \equiv 0(\bmod p')\\
&\Rightarrow (2^{\frac{p'-1}{2}} - 1)(2^{\frac{p'-1}{2}} + 1) \equiv 0(\bmod p')\\
&\Rightarrow (2^p - 1)(2^p + 1) \equiv 0(\bmod p')\\
&\Rightarrow M_p(M_p + 2) \equiv 0(\bmod p')
\end{aligned}$$

This follows that $p'|M_p$ or $p'|M_p + 2$ but not together. If p' divides both of them then this implies $p'|2$ which is impossible. This proves our theorem. □

To illustrate the above theorem lucidly let us choose $p = 5$ then $p' = 2 \times 5 + 1 = 11$. Here $M_5 = 2^5 - 1 = 31$ clearly $11 \nmid 31$ but $11|(31 + 2) = 33$. This shows the significance of the above theorem. Now if we choose $p = 11$ then $p' = 2 \times 11 + 1 = 23$. Here $M_{11} = 2^{11} - 1 = 2047$ and clearly $23|2047$ as $2047 = 23 \times 89$ but $23 \nmid (2047 + 2) = 2049$. In this two examples we have faced two cases where in the first $p'|M_p+2$ and in the second $p'|M_p$. Now the question arises: under what condition p' will divide M_p. We have discussed about that circumstances in our following theorem.

Theorem 10.4.2. *If* $p' = 2p+1$ *is prime for any prime* p *then,*

1. $p'|M_p$ *implies* $p' \equiv 1(\bmod 8)$ *or* $p' \equiv 7(\bmod 8)$
2. $p'|M_p+2$ *implies* $p' \equiv 3(\bmod 8)$ *or* $p' \equiv 5(\bmod 8)$

Proof. 1. Here $p' = 2p+1$ and $p'|M_p$ together implies $2^{\frac{p'-1}{2}} = 2^p \equiv 1(\bmod p')$. As $p'|M_p$ then from the Theorem 9.2.8 we can say that the Legendre symbol $(\frac{2}{p'}) = 1$ whenever $p' \equiv \pm 1(\bmod 8)$. Thus $p'|M_p$ implies $p' \equiv 1(\bmod 8)$ or $p' \equiv 7(\bmod 8)$.

2. Similarly if $p'|M_p+2$ then we have, $2^{\frac{p'-1}{2}} = 2^p \equiv -1(\bmod p')$, As $p'|M_p+2$ then again from the Theorem 9.2.8 we can say that the Legendre symbol $(\frac{2}{p'}) = -1$ whenever $p' \equiv \pm 3(\bmod 8)$. Thus $p'|M_p+2$ implies $p' \equiv 3(\bmod 8)$ or $p' \equiv 5(\bmod 8)$.

□

Our next corollary is an immediate consequence of above theorem.

Corollary 10.4.1. *If* p *and* $p' = 2p+1$ *both are odd primes, then* $p'|M_p$ *provided* $p \equiv 3(\bmod 4)$.

Proof. As p is odd then it is of the form $4n+1$ or $4n+3$ for any non negative integer n. Now if $p = 4n+3$ then p' becomes $8n+7$. Now from the above theorem we can say that $p'|M_p$. Also if $p = 4n+1$ then p' becomes $8n+3$. So again by the above theorem we have $p' \nmid M_p$. □

Here for an example if we choose $p = 3$ then $p' = 2\times 3+1 = 7$ both are odd. Here $M_3 = 2^3 - 1 = 7$ and obviously $7|M_3$.

Now we are going to discuss few more results on primality testing of M_p. Here we have seen under which circumstances M_p has a divisor or not. The following theorem is first among them.

Theorem 10.4.3. *If* p *is an odd prime then any prime divisor of Merenne number* M_p *is of the form* $2kp+1$ *where* k *is a positive integer.*

Proof. Let us choose p' be any prime divisor of $M_p = 2^p - 1$ then we have, $2^p \equiv 1(\bmod p')$. If 2 has the order n modulo p then by the Theorem (8.2.1) we can say that $n|p$. Here if $n = 1$ then $p'|1$ since $2^n \equiv 1(\bmod p')$ which is impossible. Thus we have $n = p$ as p is odd prime. Again from Fermat's little theorem we have,

$2^{p'-1} \equiv 1(\bmod p')$ as $\gcd(2,p') = 1$. Now again applying Theorem 8.2.1 we have seen that $n|p'-1$. But $n = p$ which shows $p|p'-1$. This implies $p'-1 = pm$ for some integer m. Therefore p' is of the form $1+pm$. Now if m is odd then p' is even which is a contradiction as p' is prime divisor of M_p. Thus we have $m = 2k$ an even number and p' is of the form $2kp+1$. □

Now we have the second following theorem to be discussed here.

Theorem 10.4.4. *If p is an odd prime then any prime divisor p' of M_p is of the form $p' \equiv \pm 1(\bmod 8)$.*

Proof. Let $p' = 2m+1$ is a prime divisor of M_p. If we choose $b = 2^{\frac{p+1}{2}}$ then $b^2 - 2 = 2^{p+1} - 2 = 2M_p \equiv 0(\bmod p')$. This implies $b^2 \equiv 2(\bmod p')$ and taking m-th power both sides of congruence we arrive at, $b^{2m} = b^{p'-1} \equiv 2^m(\bmod p')$. Here $\gcd(b,p') = 1$ as p is prime and so by Fermat's theorem $b^{p'-1} \equiv 1(\bmod p')$. Now combining these two congruences we have, $2^m \equiv 1(\bmod p')$ which shows that $p'|M_m$. Finally by Theorem 10.4.2 we have the conclusion that $p' \equiv \pm 1($ mod 8). □

From this above two theorem we can arrive at a conclusion that these two theorems can be used to decide whether a Mersenne number prime or not. Following examples are illustration of this fact.

Example 10.4.2. *Let us consider $M_{11} = 2^{11} - 1 = 2047$ and the prime factors of M_{11} are less than $\sqrt{M_{11}} = \sqrt{2047} = 45.24$. But the prime divisors here of the form $22k+1$ for any positive integer k. So the integers are 23 and 45 less than $\sqrt{M_{11}}$. We can check that $23|2047$ asserting that M_{11} is composite number. Again if we choose $M_{13} = 2^{13} - 1 = 8191$ and the prime factors of M_{13} are less than $\sqrt{M_{15}} = \sqrt{8191} = 90.504$. They are of the form $26k+1$ for $k > 0$. So the numbers are $27, 53$ and 79. Here 53 and 79 are the primes but they does not divide M_{13}. So M_{13} is a prime.*

It's deserve mentioning, that since 1914 first 12 Mersenne primes (hence, 12 perfect numbers) had been known. The last Mersenne prime(11th one), M_{89} was discovered independently in 1911 by Powers and Cunningham. In 1876 Lucas founded the prime M_{127}, the largest prime for the next 75 years.

Because there are special primality tests for Mersenne numbers, it has been possible to determine whether extremely large Mersenne numbers are prime. Following is one such primality test. This test, commonly known as The Lucas-Lehmer Test, has been extensively used to find the largest known Mersenne primes, which are the largest known primes. The proof of this test is beyond the scope of this book but may be found in Lenstra [] and Sierpinski [].

Statement 10.4.1. ***Lucas-Lehmer Test:*** *Let p be a prime and let* $M_p = 2p-1$ *denote the p-th Mersenne number. Define a sequence of integers recursively by setting* $r_1 = 4$*, and for* $k \geq 2$*,*

$$r_k \equiv r_{k-1}^2 - 2 (\bmod M_p), \; 0 \leq r_k < M_p.$$

Then, M_p *is prime if and only if* $r_{p-1} \equiv 0 (\bmod M_p)$*.*

The following example will illustrate the application of the Lucas-Lehmer Test:

Example 10.4.3. *Let us consider the Mersenne number* $M_7 = 2^7 - 1 = 127$*. Then* $r_1 = 4$ *imply* $r_2 \equiv r_1^2 - 2 \equiv 14 (\bmod 127)$*. Now* $r_3 \equiv r_2^2 - 2 = 194 \equiv 67 (\bmod 127)$*,* $r_4 \equiv r_3^2 - 2 = 4487 \equiv 42 (\bmod 127)$*,*$r_5 \equiv r_4^2 - 2 \equiv 111 (\bmod 127)$ *and* $r_6 \equiv r_5^2 - 2 \equiv 0 (\bmod 127)$*. Thus we can conclude that* M_7 *is prime.*

Various activities has been directed towards the discovery of Mersenne primes, especially since each new Mersenne prime discovered has become the largest prime known, and for each new Mersenne prime, there exist a new perfect number. At the present time, a total of 29 Mersenne primes are known and these include all Mersenne primes M_p with $p < 62981$ and with $75000 < p < 100000$. The following table illustrates the list of known Mersenne Primes.

p	Number of decimal digits in M_p	Date of Discovery
2	1	Ancient Times
3	1	Ancient Times
5	2	Ancient Times
7	3	Ancient Times
13	4	Mid 15th century
17	6	1603
19	6	1603
31	10	1772
61	19	1883
89	27	1911
107	33	1914
127	39	1876
521	157	1952
607	183	1952
1279	386	1952
2203	664	1956
2281	687	1952
3217	969	1957
4253	1281	1961
4423	1332	1961
9689	2917	1963
9941	2993	1963
11213	3376	1963
19937	6002	1971
21701	6533	1978
23209	6987	1979
44497	13395	1979
86243	25962	1983
132049	39751	1983
216091	65050	1985.

Many mathematicians believe that there are infinitely many Mersenne primes, but a proof of this seems to be an open problem. As p increases, known Mersenne primes M_p clearly become more scarce. It has been hypothecated that about two primes M_p should be expected for all primes p in an interval $x < p < 2x$.

One of the renowned problems of number theory is whether there exist any odd perfect numbers. Although no odd perfect number has been produced so far. But, it is possible to find certain conditions for the existence of odd perfect numbers. The oldest of these was due to Euler, is reflected in the form of the following theorem:

Theorem 10.4.5. *If n is an odd perfect number, then $n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$ where p_i's are distinct odd primes and $p_1 \equiv k_1 \equiv 1(\bmod 4)$.*

Proof. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of n. As n is perfect so we have,

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_1^{k_1}).$$

Now n is odd imply $n \equiv \pm 1(\bmod 4)$ then $\sigma(n) = 2n \equiv 2(\bmod 4)$. This shows that $\sigma(n)$ is divisible by 2 but not by 4. Thus one of $\sigma(p_i^{k_i})$ is even and the rest of are odd. Let us choose $\sigma(p_1^{k_1})$ is even. As p_i's are odd primes then $p_i \equiv \pm 1(\bmod 4)$. Then for $p_i \equiv -1(\bmod 4)$ we have,

$$\begin{aligned} \sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\ &\equiv 1 + (-1) + \cdots + (-1)^{k_i} (\bmod 4) \end{aligned}$$

Therefore $\sigma(p_i^{k_i}) \equiv 0(\bmod 4)$ if k_i is odd and $\sigma(p_i^{k_i}) \equiv 1(\bmod 4)$ if k_i is even. Here $\sigma(n) \equiv 2(\bmod 4)$ implies $\sigma(p_1^{k_1}) \equiv 2(\bmod 4)$ if $\sigma(p_i^{k_i}) \equiv 1(\bmod 4)$ $(i = 2, 3, \cdots r)$. Otherwise $\sigma(p_i^{k_i}) \equiv 0(\bmod 4)$ signifies that 4 divides $\sigma(p_i^{k_i})$ which is not possible. Now here $\sigma(p_1^{k_1}) \equiv 2(\bmod 4)$ gives us $k_1 \equiv 1(\bmod 4)$. Also for other values of i as $\sigma(p_i^{k_i})$'s are odd the $\sigma(p_i^{k_i}) \equiv \pm 1(\bmod 4)$. This also implies $k_i \equiv 0(\bmod 4)$ or $k_i \equiv 2(\bmod 4)$. Thus in any cases k_i's are even integer for $i = 2, 3, \cdots r$. This proves the theorem. ☐

Now in the following corollary we have given the form of an odd perfect number. This is also an immediate consequence of above theorem.

Corollary 10.4.2. *If n is an odd perfect number then it is of the form $n = p^t k^2$, where p is an odd prime with $p \nmid k$ and $p \equiv t \equiv 1(\bmod 4)$. Then we have $n \equiv 1(\bmod 4)$ also.*

Proof. From the above theorem it follows that,

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = p_1^{k_1} (p_2^{j_2} \cdots p_r^{j_r})^2 = p^t k^2, \text{ where } p_1 = p, k_1 = t \ \& \ k = p_2^{j_2} \cdots p_r^{j_r}.$$

As $p \equiv 1(\bmod 4)$ then we have $p^t \equiv 1(\bmod 4)$. Also k is odd imply $k \equiv 1(\bmod 4)$ or $k \equiv 3(\bmod 4)$. Thus in any case we have $k^2 \equiv 1(\bmod 4)$. Then it follows that $n = p^t k^2 \equiv 1 \cdot 1 \equiv 1(\bmod 4)$. ☐

10.5 Worked out Exercises

Problem 10.5.1. *Any two distinct Mersenne numbers are coprime.*

Solution 10.5.1. *Let* p, q *be two distinct primes where* $q > p$. *Note that* $gcd(p, q) = 1$. *It can also be obtained by Euclid's algorithm. Then for any integer* k *we have*

$$\begin{aligned} q &= kp + r_1, \\ p &= k_1 r_1 + r_2, \\ r_1 &= k_2 r_2 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1} k_{n-1} + r_n, \\ &= r_{n-1} k_{n-1} + 1. \end{aligned}$$

Let l *be the common divisor of* $M_p = 2^p - 1$ *and* $M_q = 2^q - 1$. *Then we have,*

$$\begin{aligned} &\therefore\ l \big| [(2^q - 1) - 2^{q-p}(2^p - 1)], \\ &\Rightarrow l \big| (2^{q-p} - 1), \\ &\Rightarrow l \big| [(2^{q-p} - 1) - 2^{q-2p}(2^p - 1)], \\ &\Rightarrow l \big| (2^{q-2p} - 1), \\ &\quad \vdots \\ &\Rightarrow l \big| (2^{q-kp} - 1), \\ &\Rightarrow l \big| (2^{r_1} - 1), \\ &\quad \vdots \\ &\Rightarrow l \big| (2^{r_n} - 1), \\ &\Rightarrow l = 1.\ \therefore\ \gcd(M_p, M_q) = 1. \end{aligned}$$

Problem 10.5.2. *Show that the Mersenne number* $M_{13} = 2^{13} - 1$ *is prime and hence the integer* $2^{12}(2^{13} - 1)$ *is perfect.*

Solution 10.5.2. *Note that the Mersenne number* $M_{13} = 2^{13} - 1$ *has prime divisor of the form* $2k \cdot 13 + 1$*[see Theorem 10.4.3]. Applying Example 10.4.2,* *we can say that* M_{13} *is prime. Claim:* $n = 2^{12}(2^{13}-1)$ *is perfect. Thus,*

$$\begin{aligned}\sigma(n) &= \sigma(2^{12}M_{13})\\ &= \sigma(2^{12})\sigma(M_{13})\\ &= (2^{13}-1)(2^{13}-1+1)\\ &= 2^{13}(2^{13}-1) = 2n.\end{aligned}$$

Hence the integer $2^{12}(2^{13}-1)$ *is perfect.*

Problem 10.5.3. *Prove that the Mersenne number* M_{29} *is composite.*

Solution 10.5.3. *The given Mersenne number* $M_{29} = 2^{29}-1$ *has the prime divisor of the form* $2k \cdot 29 + 1$*, for any integer* k*. From* $\sqrt{M_{29}} < 23171$*, we obtain few possible divisors viz* $59, 117, 233$*. Amongst them we can verify that* $233 | M_{29}$*, which implies* M_{29} *is a composite number.*

Problem 10.5.4. *A pair of integers* m *and* n *is said to be amicable numbers if* $\sigma(m) = m + n = \sigma(n)$ *holds. Now for such pair* m *and* n *prove that,*

$$\left(\sum_{d|m}\frac{1}{d}\right)^{-1} + \left(\sum_{d|n}\frac{1}{d}\right)^{-1} = 1.$$

Solution 10.5.4. *Note that* $\sum_{d|m}\frac{1}{d} = \sum_{d|m}\frac{d}{m}$ *and* $\sum_{d|n}\frac{1}{d} = \sum_{d|n}\frac{d}{n}$*. Combining we get,*

$$\begin{aligned}\left(\sum_{d|m}\frac{1}{d}\right)^{-1} + \left(\sum_{d|n}\frac{1}{d}\right)^{-1} &= \frac{n}{\sigma(n)} + \frac{m}{\sigma(m)}\\ &= \frac{m+n}{m+n}\ [\because \sigma(m) = \sigma(n) = m+n]\\ &= 1.\end{aligned}$$

Problem 10.5.5. *Show that for any odd prime* p *neither* p *nor* p^2 *can be one of an amicable pair.*

Solution 10.5.5. *Let* p *be an arbitrary prime. Then* $\sigma(p) = p + 1$*. Let* p *and* p^2 *be the amicable pair. Then* $\sigma(p) = p + 1 = \sigma(p^2) = \frac{p^3-1}{p-1}$*. Thus* $p^2 - 1 = p^3 - 1 \Rightarrow p = 1$*. This is not possible. So neither* p *nor* p^2 *can be one of the amicable pair.*

Problem 10.5.6. *Prove that for any odd prime* p *if* $n = pa^2$ *is an odd perfect number, then* $n \equiv p (\text{mod } 8)$*.*

Solution 10.5.6. *Assume that* $n = pa^2$ *is an odd perfect number. Then* a *is an odd integer. Thus* a *is of the form* $4k \pm 1$. *Now* $a^2 = (4k \pm 1)^2 = 16k^2 \pm 8k + 1 \equiv 1(\bmod 8)$. $\therefore n = pa^2 \equiv p(\bmod 8)$.

Problem 10.5.7. *Use the Lucas-Lehmer test to determine whether the Mersenne number* M_{11} *is prime or not.*

Solution 10.5.7. *Here the Mersenne number is* $M_{11} = 2^{11} - 1 = 2047$. *Then* $r_1 = 4 \Rightarrow r_2 \equiv r_1^2 - 2 = 14(\bmod 2047)$. *Now* $r_3 \equiv r_2^2 - 2 = 195(\bmod 2047)$ *and* $r_4 \equiv r_3^2 - 2 = 1177(\bmod 2047)$. *So continuing this way(Do it!) we find* $r_{10} \not\equiv 0(\bmod M_{11})$. *So* M_{11} *is not a prime.*

Problem 10.5.8. *If the integer* $n > 1$ *is a product of distinct Mersenne primes, prove that* $\sigma(n) = 2^k$ *for some integer* k.

Solution 10.5.8. *Let* $M_p = 2^p - 1$ *and* $M_q = 2^q - 1$ *be the distinct Mersenne primes and* $n = M_pM_q$. *Then*

$$\begin{aligned}\sigma(n) &= \sigma(M_p)\sigma(M_q)\\ &= (M_p + 1)(M_q + 1)\\ &= 2^p \cdot 2^q = 2^{p+q} = 2^k.\end{aligned}$$

$\therefore \sigma(n)$ *is of the form* 2^k *for any integer* k.

Problem 10.5.9. *If* p *is an odd prime of the form* $4k + 3$ *for any integer* k *and* $q = 2p + 1$ *be another prime then prove that* q *divides the Mersenne number* $M_p = 2^p - 1$.

Solution 10.5.9. *Here* p *is of the form* $4k+3$. *Then* $q = 2p+1 = 2(4k+3)+1 = 8k + 7$. *By Theorem 9.2.8 we have,* $(\frac{2}{q}) = 1$ *as* $q \equiv 7(\bmod 8)$. *Moreover, by Euler's Criterion we see that* $2^{\frac{q-1}{2}} \equiv 2^p \equiv 1(\bmod q)$. *This shows that* $q\big|(2^p - 1)$.

Problem 10.5.10. *Prove that if* n *is a positive integer and* $2n + 1$ *is prime, and if* $n \equiv 0(mod4)$ *or* $n \equiv 3(\bmod 4)$ *then* $2n + 1$ *divides the Mersenne number* $M_n = 2^n - 1$, *while if* $n \equiv 1(\bmod 4)$ *or* $n \equiv 2(\bmod 4)$, *then* $2n + 1$ *divides* $M_n + 2 = 2^n + 1$.

Solution 10.5.10. *If* $n \equiv 0(mod4)$ *or* $n \equiv 3(\bmod 4)$, *then* $2n + 1 \equiv 1(\bmod 8)$ *or* $2n+1 \equiv 7(\bmod 8)$ *respectively. In both these cases, we have* $(\frac{2}{2n+1}) = 1$*(refer to Theorem 9.2.8). By Euler's Criterion, we get* $2^{\frac{2n+1-1}{2}} = 2^n \equiv 1(\bmod 2n+1)$. *This proves that* $2n + 1\big|(2^n - 1)$.

Furthermore, if $n \equiv 1(mod4)$ *or* $n \equiv 2(\bmod 4)$, *then* $2n + 1 \equiv 3(\bmod 8)$ *or* $2n + 1 \equiv 5(\bmod 8)$ *respectively. In both these cases, we obtain* $\frac{2}{2n+1} = -1$*(refer to Theorem 9.2.8). By Euler's Criterion,* $2^{\frac{2n+1-1}{2}} = 2^n \equiv -1(\bmod 2n+1)$. *This yields* $2n + 1\big|(2^n + 1)$.

10.6 Fermat Numbers

In this section our discussion is based on particular numbers of the form $F_n = 2^{2^n} + 1$ where n is a non negative integer. They are called Fermat numbers, named after the French mathematician Pierre de Fermat who first studied numbers of this form. Here we have also discussed few basic properties and primality of Fermat numbers. Fermat's first conjecture was that all the numbers of these type were prime. But in 1732 Euler showed that the number $F_5 = 2^{2^5} + 1$ is composite. Then it become a question whether there are infinitely many prime of this form or not. Thus to start our discussion we have given the following definition of Fermat numbers as well as Fermat primes.

Definition 10.6.1. *An integer is of the form* $F_n = 2^{2^n} + 1,\ n \geq 0$ *is called Fermat number. If* F_n *is prime then it is called Fermat prime.*

For example we can see that the first five Fermat numbers $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257$ and $F_4 = 65,537$ all are primes. But the conjecture that Fermat numbers are primes fails to F_5. Here $F_5 = 2^{2^5} + 1 = 641 \times 6700417$ is composite. In fact we have an elementary proof that $641 | F_5$ due to G.Bennet.

Theorem 10.6.1. *The Fermat number* F_5 *is divisible by* 641.

Proof. Let us choose $u = 2^7$ and $v = 5$ then we have, $1 + uv = 1 + 2^7 \cdot 5 = 641$. It is seen that , $1 + uv - v^4 = 1 + v(u - v^3) = 1 + (2^7 - 5^3)v = 1 + 3v = 2^4$. Now

$$\begin{aligned} F_5 &= 2^{2^5} + 1 \\ &= 2^4 \cdot 2^{28} + 1 \\ &= 2^4 \cdot u^4 + 1 \\ &= (1 + uv - v^4)u^4 + 1 \\ &= (1 + uv)[u^4 + (1 - uv)(1 + u^2v^2)] \end{aligned}$$

This shows that 641 divides F_5 as $1 + uv = 641$. □

We are now going to prove some basic properties of Fermat numbers in our next theorem.

Theorem 10.6.2.
1. *For* $n \geq 1,\ F_n = (F_{n-1} - 1)^2 + 1$
2. *For* $n \geq 1,\ F_n - 2 = F_0F_1 \cdots F_{n-1}$
3. *For* $n \geq 2,\ F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$
4. *For* $n \geq 2,\ F_n - F_{n-1} = 2^{2^{n-1}} F_0F_1 \cdots F_{n-2}$

Proof.

1. $(F_{n-1}-1)^2+1=(2^{2^{n-1}}+1-1)^2+1=2^{2^n}+1=F_n$.

2. We have to prove this result by principle of mathematical induction. When $n=1$, we have $F_1-2=5-2=3=F_0$. Let the result is true for $n=k$ then, $F_k-2=F_0F_1\cdots F_{k-1}$. Now,

$$\begin{aligned} F_0F_1\cdots F_k+2 &= (F_k-2)F_k+2 \\ &= (2^{2^k}-1)(2^{2^k}+1)+2 \\ &= 2^{2^{k+1}}+1 \\ &= F_{k+1} \end{aligned}$$

$\therefore$, $F_{k+1}-2=F_0F_1\cdots F_k$. Thus the result is true for $n=k+1$. So by the principle of mathematical induction the result is true.

3. $$\begin{aligned} F_{n-1}^2-2(F_{n-2}-1)^2 &= (2^{2^{n-1}}+1)^2-2(2^{2^{n-2}})^2 \\ &= 2^{2^n}+2\cdot 2^{2^{n-1}}+1-2\cdot 2^{2^{n-1}} \\ &= 2^{2^n}+1 \\ &= F_n,\ n\geq 2 \end{aligned}$$

4. We have to prove this result by principle of mathematical induction. When $n=2$, we have $F_1+2^2\cdot F_0=5+2^2\cdot 3=17=F_2$. Now let us assume the result is true for $n=k$. Then we have $F_k=F_{k-1}+2^{2^{k-1}}F_0F_1\cdots F_{k-2}$. Now,

$$\begin{aligned} F_k+2^{2^k}F_0F_1\cdots F_{k-1} &= F_k+2^{2^{k-1}}(2^{2^{k-1}}F_0F_1\cdots F_{k-2})F_{k-1} \\ &= F_k+2^{2^{k-1}}(F_k-F_{k-1})F_{k-1} \\ &= (2^{2^k}+1)+2^{2^{k-1}}(2^{2^k}-2^{2^{k-1}}(2^{2^{k-1}}+1) \\ &= (2^{2^k}+1)+2^{2^k}(2^{2^k}-1) \\ &= 1+2^{2^{k+1}} \\ &= F_{k+1} \end{aligned}$$

Thus the result is true for $n=k+1$. So by the principle of mathematical induction the result is true.

□

We are now going to exhibit an important property of Fermat number.

Theorem 10.6.3. *Let m and n be distinct non negative integers with $m < n$. Then the Fermat numbers F_n and F_m are relatively prime.*

Proof. From the Theorem 10.6.2 we have, $F_n - 2 = F_0F_1 \cdots F_m \cdots F_{n-1}$ $(m < n)$. Let us assume d is a common divisor of F_m and F_n then $d|F_m$ and $d|F_n - 2$. Now combining together we have $d|2$. This is possible only when $d = 1$ or $d = 2$. As F_m and F_n are odd then $d = 2$ is not possible. Thus we have $d = 1$. This proves the theorem. ☐

This theorem leads us to the fact that there are infinitely many primes. Since $\gcd(F_m, F_n) = 1$ then every Fermat number F_n has a prime factor p_n(say) which imply $p_m \neq p_n$ whenever $m \neq n$. Now the following theorem we have given another way on primality testing of F_n. This theorem is called Pepin Test due to T.Pepin.

Theorem 10.6.4. *(Pepin's Test):For any $m \geq 1$ the Fermat number $F_m = 2^{2^m} + 1$ is prime if and only if $3^{\frac{F_m-1}{2}} \equiv -1 (\bmod F_m)$ holds.*

Proof. Let us choose that the congruence, $3^{\frac{F_m-1}{2}} \equiv -1 (\bmod F_m)$ holds. We are to show that F_m is prime. Now squaring both sides of the congruence, we have $3^{F_m-1} \equiv 1 (\bmod F_m)$. Let us choose F_m is composite and p be any prime factor of F_m. Then we can say that, $3^{F_m-1} \equiv 1 (\bmod p)$. Let k be the order of 3 modulo p then by the Theorem 8.2.1 we have $k|(F_m - 1)$. This implies that $k|2^{2^m}$ and k must be a power of 2. Let $k = 2^r$ for any $r \leq 2^{m-1}$ then squaring both sides of $3^k \equiv 1 (\bmod p)$ repeatedly yields that, $3^{2^{2^{m-1}}} \equiv 1 (\bmod p)$. This implies that $3^{\frac{F_m-1}{2}} \equiv 1 (\bmod p)$. Then from the given condition it follows that $1 \equiv -1 (\bmod p)$. This shows that $p = 2$ which is a contradiction. Thus the only possiblity is $k = 2^{2^m} = F_m - 1$. Since $k = F_m - 1 \leq p - 1$ and $p|F_m$ then we have $p = F_m$ and consequently F_m becomes a prime. Conversely if $F_m = 2^{2^m} + 1$ is prime for $m \geq 1$, then by the law of quadratic reciprocity we have, $(\frac{3}{F_m}) = (\frac{F_m}{3}) = (\frac{2}{3}) = -1$, since $F_m \equiv (-1)^{2^m} + 1 \equiv 2 (\bmod 3)$. Now by Euler's Criterion we have, $(\frac{3}{F_m}) \equiv 3^{\frac{F_m-1}{2}} (\bmod F_m)$. Now together gives us $3^{\frac{F_m-1}{2}} \equiv -1 (\bmod F_m)$. This proves the theorem. ☐

Example 10.6.1. *Let us choose $m = 1$, then $F_1 = 2^{2^1} + 1 = 5$ and $3^{\frac{F_1-1}{2}} = 3^2 = 9 \equiv -1 (\bmod 5)$. So by Pepin's Test we have F_1 is prime. Similarly taking $m = 2$ by Pepin's test we can see that $F_2 = 17$ is prime.*

The following is our final theorem of this section where we have shown an important aspect on finding the divisor of a perfect number. In the year 1747, Euler established that every prime factor of F_m is of the form $k \cdot 2^{n+1} + 1$ then after 100 years later in 1879 Edouard Lucas improved this result. So from there we have this following theorem.

Theorem 10.6.5. *For $m \geq 2$, any prime divisor p of a Fermat number F_m is of the form $p = n \cdot 2^{m+2} + 1$.*

Proof. Let p be a prime divisor of F_m then, $2^{2^m} \equiv -1 (\bmod p)$. Now squaring both sides of the congruence we have $2^{2^{m+1}} \equiv 1 (\bmod p)$. Let k be the order of 2 modulo p then we have from the Theorem 8.2.1, $k | 2^{m+1}$. Here k is not of the form 2^r where $1 \leq r \leq m$, otherwise this leads to $2^{2^m} \equiv 1 (\bmod p)$. This is a contradiction as $1 \equiv -1 (\bmod p)$ imply $p = 2$. So k is of the form 2^{m+1}. Since order of 2 modulo p divides $\phi(p) = p - 1$, then $2^{m+1} | p - 1$. Thus $m \geq 2$ and $2^{m+1} | p - 1$ together shows that $p \equiv 1 (\bmod 8)$. So by Theorem(9.2.8) we have the Legendre symbol $(\frac{2}{p}) = 1$. Also by Euler's Criterion, $2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) = 1($ mod $p)$. Thus from the Theorem 8.2.1 we have $k = 2^{m+1} | \frac{(p-1)}{2}$. So we obtain $p = n \cdot 2^{m+2} + 1$ for some integer n. □

To illustrate this theorem let us choose $F_3 = 2^{2^3} + 1 = 257$ then any prime factor of F_3 is less than $\sqrt{F_3}$. Now by last theorem any prime factor of F_3 is of the form $k \cdot 2^5 + 1 = 32k + 1$ for any integer k. As $p > 1$ then there is no such integer k and hence F_3 is prime.

Finally we conclude this section with a geometrical aspects of Fermat numbers. A Fermat number $F_m = 2^{2^m} + 1$ for $m \geq 1$ is called a Fermat prime if m is prime. Now if we think each value of a Fermat prime as a unit square then those unit squares can be arranged as a square whose length of each side is $2^{2^{m-1}}$ and an extra unit square. For example if we choose $m = 2$ then $F_2 = 2^{2^2} + 1 = 17$. Now here we have 17 unit squares and they can be arranged as a square of side length $2^{2^{2-1}} = 4$ and an extra unit square. This has been shown in below figure.

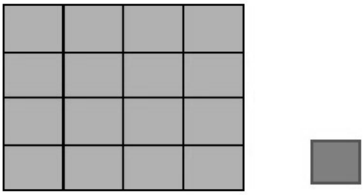


Figure 10.2:

Similarly for $F_3 = 2^{2^3} + 1 = 257 = 16^2 + 1$ we have a square whose side length is 16 and an extra unit square. Here determining a Fermat number is composite or not is equivalent to arrange all the unit squares as a rectangle or not. If we can't arrange them as a rectangle then it is prime otherwise composite number. See the figure below for $F_2 = 17$.

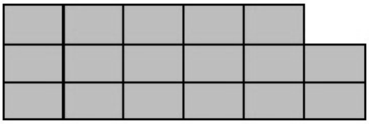


Figure 10.3:

10.7 Worked out Exercises

Problem 10.7.1. *Show that* $2^{2^n} + 5$ *is composite for each integer* $n (> 0)$.

Solution 10.7.1. *For any positive integer* n, 2^n *is even. Then we have,* $2^{2^n} \equiv 1 (\bmod 3)$. *This shows that,* $2^{2^n} + 5 \equiv 1 + 5 \equiv 0 (\bmod 3)$. *Since* $3 \big| 2^{2^n} + 5$, *therefore* $2^{2^n} + 5$ *is composite.*

Problem 10.7.2. *Prove that every Fermat number* F_n *is either a prime or a pseudoprime.*

Solution 10.7.2. *We need to verify, if* F_n *is composite then it is pseudoprime. For that, we need to prove* $(2^{2^n})^{2^n+1} \equiv 2 (\bmod F_n)$. *We know that,*

$$\begin{aligned} & 2^{2^n} \equiv -1 (\bmod F_n) \\ \Rightarrow\ & (2^{2^n})^{2^{2^n}-n} \equiv (-1)^{2^{2^n}-n} (\bmod F_n) \\ \Rightarrow\ & 2^{2^{2^n}} \equiv 1 (\bmod F_n) \\ \Rightarrow\ & (2^{2^n})^{2^n+1} \equiv 2 (\bmod F_n). \end{aligned}$$

Problem 10.7.3. *Taking fourth powers of congruences on* $5 \cdot 2^7 \equiv -1 (\bmod 641)$ *deduce that* $2^{32} + 1 \equiv 0 (\bmod 641)$ *and hence* $641 | F_5$.

Solution 10.7.3. *Note that* $5 \cdot 2^7 \equiv -1(\text{mod } 641)$*. Then*

$$\begin{aligned} 5^4 \cdot (2^7)^4 &\equiv (-1)^4(\text{ mod } 641) \\ \Rightarrow 625 \cdot 2^{28} &\equiv 1(\text{ mod } 641) \\ \Rightarrow -16 \cdot 2^{28} &\equiv 1(\text{ mod } 641) \\ \Rightarrow -2^{32} &\equiv 1(\text{ mod } 641). \end{aligned}$$

This implies that $641|2^{32} + 1 = 2^{2^5} + 1 = F_5$.

Problem 10.7.4. *For* $n \geq 2$*, show that the last digit of the Fermat number* $F_n = 2^{2^n} + 1$ *is* 7.

Solution 10.7.4. *First, we prove* $2^{2^n} \equiv 6(\text{mod } 10)$ *for* $n \geq 2$*. For this, apply principle of mathematical induction. For* $n = 2$*, we have* $2^{2^2} = 2^4 = 16 \equiv 6(\text{mod } 10)$*. Thus the statement is true for* $n = 2$*. Let the result be true for* $n = k$*. To prove the result for* $n = k+1$*, let us take* $2^{2^{k+1}} = 2^4 \cdot 2^{2^k} \equiv 16 \cdot 6 \equiv 6(\text{mod } 10)$*. So the result is true for* $n = k+1$*. Thus we have* $2^{2^n} + 1 \equiv 7(\text{mod } 10)$*. Therefore the unit digit is* 7.

Problem 10.7.5. *For* $n \geq 1$*, prove that* $\gcd(F_n, n) = 1$.

Solution 10.7.5. *Let us assume that* $d = \gcd(F_n, n)$ *and* p *be any prime divisor of* d*. Then* $p|F_n$ *and* $p|n$*. Taking into consideration Theorem 10.6.5,* p *is of the form and* $p = k \cdot 2^{n+2} + 1$*. As* $p|n$*, then we have* $p = k \cdot 2^{n+2} + 1 \leq n$*. This leads to a contradiction. Thus* $\gcd(F_n, n) = 1$.

Problem 10.7.6. *For any odd integer* n*, show that* $3|2^n + 1$.

Solution 10.7.6. *Let us assume* n *is odd. Then it is of the form* $2k + 1$ *for any positive integer* k*. This follows that* $2^n = 2^{2k+1} = 2 \cdot 4^k$*. Claim:* $2 \cdot 4^k \equiv 2(\text{mod } 3)$*. To fulfill the claim, apply principle of mathematical induction. Let us take* $k = 1$*. Then* $2 \cdot 4 = 8 \equiv 2(\text{mod } 3)$*. So the result is true for* $k = 1$*. Let the result be true for* $k = t$*. This follows* $2 \cdot 4^t \equiv 2(\text{mod } 3)$*. Let* $k = t + 1$*. Then we have*

$$\begin{aligned} 2 \cdot 4^{t+1} &= 4 \cdot 2 \cdot 4^t \\ &\equiv 4 \cdot 2 \equiv 2(\text{ mod } 3). \end{aligned}$$

So the result is true for $k = t + 1$*. Thus by principle of mathematical induction, the result is true for all integers* n*. Therefore* $2 \cdot 4^k \equiv 2(\text{mod } 3) \Rightarrow 2 \cdot 4^k \equiv -1(\text{mod } 3)$*. This proves* $3|(2^n + 1)$.

Problem 10.7.7. *For any Fermat number* $F_n = 2^{2^n} + 1$*, establish that* $F_n \equiv 5(\text{mod } 9)$ *or* $F_n \equiv 8(\text{mod } 9)$ *according as* n *is odd or even.*

Solution 10.7.7. *Let* $F_n = 2^{2^n} + 1$ *be the arbitrary Fermat number for* $n > 0$*. Now* $2^n \equiv (-1)^n (\text{mod } 3)$ *implies that if* n *is odd then* 2^n *is of the form* $3k + 2$ *where* k *is even and if* n *is even then* 2^n *is of the form* $3k' + 1$ *for some odd integer* k'*.*

If n *is odd then we have,*

$$2^{2^n} + 1 = 2^{3k+2} + 1 \equiv 4 + 1 \equiv 5(\text{ mod } 9).$$

If n *is even then we have,*

$$2^{2^n} + 1 = 2^{3k'+1} + 1 \equiv (-1) \cdot 2 + 1 \equiv -1 \equiv 8(\text{ mod } 9).$$

Problem 10.7.8. *Use Pepin's test to show the Fermat number 257 is prime.*

Solution 10.7.8. *Note that* $F_3 = 2^{2^3} + 1 = 257$*. So* $3^{\frac{F_3-1}{2}} = 3^{128}$*. Moreover,* $3^{128} = (3^8)^{16} \equiv 136^{16} \equiv 64^4 \equiv 241^2 \equiv 256 \equiv -1(\text{mod } 257)$*. Then by Pepin's Test* $F_3 = 257$ *is prime.*

Problem 10.7.9. *From Pepin's test, conclude that* 3 *is a primitive root of every Fermat prime.*

Solution 10.7.9. *Let* $F_p = 2^{2^p} + 1$ *is prime. Then* $\phi(F_p) = 2^{2^p}$*. So order of* 3 *modulo* F_p *is a power of* 2*, say* 2^k*. Then* $3^{2^p} = 3^{2^k \cdot 2^{p-k}} \equiv 1(\text{mod } F_p)$ *if* $p \geq k$*. By Pepin's Test, we have* $3^{\frac{F_p-1}{2}} \equiv -1(\text{mod } F_p)$*. Then* $3^{F_p-1} \equiv 1(\text{mod } F_p)$*. So order of* 3 *modulo* F_p *is* $\phi(F_p)$*. This proves that* 3 *is the primitive root for every prime as p is arbitrary.*

10.8 Exercises:

1. Verify that a perfect square cannot be a perfect number.

2. Establish the following assertions concerning k-perfect number:
   (a)If n is a 3-perfect number and $3 \nmid n$, then $3n$ is 4-perfect.
   (b)If n is a 5-perfect number and $5 \nmid n$, then $5n$ is 6-perfect.

3. Prove that if $n \neq 28$ is an even perfect number, then $n \equiv 1$ or $-1(\text{mod } 7)$.

4. Prove that if $2^k - 1$ is prime, then the sum

   $$2^{k-l} + 2^k + 2^{k+l} + \cdots + 2^{2k-2}$$

   will yield a perfect number. For instance, $2^3 - 1$ is prime and $2^2 + 2^3 + 2^4 = 28$, which is perfect.

5. (a) Show that any divisor of a deficient or perfect number is deficient.
   (b) Show that any multiple of an abundant or perfect number is abundant.

6. (a) Show that 16 is a superperfect number.
   (b) Show that for an odd prime p if $n = p^2$, then n is not super perfect.

7. Prove that the Mersenne number M_{19} is a prime; hence, the integer $n = 2^{18}(2^{19} - 1)$ is perfect.

8. If m and n are an amicable pair, with m even and n odd, then n is a perfect square.

9. Show that Any odd perfect number n can be represented in the form $n = pa^2$, where p is a prime.

10. If n is an odd perfect number, prove that n has at least three distinct prime factors.

11. Use the Lucas-Lehmer test to determine whether the Mersenne numbers M_3 and M_{13} are prime or not.

12. Find the smallest prime divisor $q > 3$ of each of the integers $2^{29} + 1$ and $2^{41} + 1$.

13. For any prime $p > 3$, prove that $\frac{1}{3}(2^p + 1)$ is not divisible by 3.

14. Establish that any Fermat prime F_n can be written as the difference of two squares, but not of two cubes.

15. Prove that if n is odd pseudoprime then the Mersenne number M_n is also pseudoprime.

11

Continued Fractions

> *"If equations are trains threading the landscape of numbers, then no train stops at pi."*
>
> – Richard Preston

11.1 Introduction

Being a natural object, continued fractions appear in many areas of Mathematics, sometimes in an unexpected way. The old name of continued fraction was "anthyphaeiretic ratios", which the Dutch mathematician and astronomer in 1687 made the first practical application explaining how to use convergents to find the best rational approximations for ratios. To build a mechanical planetarium, motivated him to do so. Later on, many renowned mathematicians including Euler, Jacobi, Gauss and Cauchy get attracted to continued fractions. Continued fractions find its applications in some areas of contemporary Mathematics. The application of continued fraction lies in the cryptography, to explain a kind of attack on the RSA system. Nowadays, there are mathematicians who continue to develop the theory on continued fractions.

The sections of the chapter starts with finite continued fractions and then subsequently we move to infinite and periodic continued fractions.

11.2 Finite Continued Fractions

We commence this section with an example, by taking $\frac{137}{33}$. Applying Euclidean Algorithm on $\frac{137}{33}$ yields

$$\begin{aligned} 137 &= 4\cdot 33 + 5 \\ 33 &= 6\cdot 5 + 3 \\ 5 &= 1\cdot 3 + 2 \\ 3 &= 1\cdot 2 + 1. \end{aligned}$$

Dividing both sides of every equations by the divisor of that equation, we obtain

$$\begin{aligned} \frac{137}{33} &= 4 + \frac{5}{33} = 4 + \frac{1}{\frac{33}{5}} \\ \frac{33}{5} &= 6 + \frac{3}{5} = 6 + \frac{1}{\frac{5}{3}} \\ \frac{5}{3} &= 1 + \frac{2}{3} = 1 + \frac{1}{\frac{3}{2}} \\ \frac{3}{2} &= 1 + \frac{1}{2}. \end{aligned}$$

Combining we get,

$$\frac{137}{33} = 4 + \frac{5}{33} = 4 + \frac{1}{6 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}}}.$$

The foregoing expression in this sequence of equations is a simple finite continued fraction of $\frac{137}{33}$. This motivates us to start with the following definition.

Definition 11.2.1. *A finite continued fraction is an expression of the form*

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{\ddots + b_{n-1} + \cfrac{1}{b_n}}},$$

where $b_0, b_1, b_3, \ldots, b_n$ *are real numbers with* $b_1, b_3, \ldots, b_n$ *being positive. The real quantities* $b_1, b_3, \ldots, b_n$ *are known to be partial quotients (also known as partial denominators) of the continued fraction. The continued fraction is simple (canonical) if the real numbers* $b_0, b_1, b_3, \ldots, b_n$ *are all integers. Symbolically, continued fractions are denoted by* $[b_0; b_1, b_3, \ldots, b_n]$ *to avoid writing out continued fractions.*

The first theorem of the section reflects on the representation of every finite simple continued fractions. Later on using Euclidean Algorithm, we will work on the representation of every rational number as a finite continued fraction.

Theorem 11.2.1. *Every finite simple continued fraction represents a rational number.*

Proof. Let $[b_0; b_1, b_2, b_3, \ldots, b_k]$ with $1 \leq k \leq n$ be b finite simple continued fraction. We proceed by mathematical induction on k. For $k = 1$, we have $[b_0; b_1] = b_0 + \frac{1}{b_1} = \frac{b_0 b_1 + 1}{b_1}$, a rational number. Assume the theorem is true for $k = m$. Then for $1 \leq m \leq n$, we have $[b_0; b_1, b_2, b_3, \ldots, b_m]$ is a rational number. Now for $k = m + 1$, we obtain

$$[b_0; b_1, b_2, b_3, \ldots, b_m, b_{m+1}] = b_0 + \frac{1}{[b_1; b_2, b_3, b_4, \ldots, b_m, b_{m+1}]}.$$

By induction hypothesis, $[b_1; b_2, b_3, b_4, \ldots, b_m, b_{m+1}]$ is rational which implies it can be expressed in the form $\frac{r}{s}$ with $r, s \in \mathbb{Z}$, $s \neq 0$ and $\gcd(r, s) = 1$. Thus,

$$[b_0; b_1, b_2, b_3, \ldots, b_m, b_{m+1}] = b_0 + \frac{1}{\frac{r}{s}} = b_0 + \frac{s}{r} = \frac{b_0 r + s}{r},$$

a rational number. Hence by induction method we are done. □

Theorem 11.2.2. *Any rational number can be expressed as a finite simple continued fraction.*

Proof. Let x be a rational quantity. Then $\exists\, u, v \in \mathbb{Z}$ with $v \neq 0$ and $\gcd(u, v) = 1$ such that $x = \frac{u}{v}$. Suppose $r_0 = u$ and $r_1 = v$. Then an appeal to Euclidean algorithm yields the following sequence of equations viz

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, & 0 &< r_2 < r_1. \\
r_1 &= r_2 q_2 + r_3, & 0 &< r_3 < r_2. \\
r_2 &= r_3 q_2 + r_4, & 0 &< r_4 < r_3. \\
\vdots &= \vdots \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1}, & 0 &< r_{n-1} < r_{n-2}. \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 &< r_n < r_{n-1}. \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

In the above equations, $q_2, q_3, \ldots, q_n$ are all positive integers. Rewriting the algorithm in fractional form we get,

$$\begin{aligned}
\frac{u}{v} = \frac{r_0}{r_1} &= q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}} \\
\frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}} \\
\frac{r_2}{r_3} &= q_3 + \frac{r_4}{r_3} = q_1 + \frac{1}{\frac{r_3}{r_4}} \\
\vdots &= \vdots \\
\frac{r_{n-3}}{r_{n-2}} &= q_{n-2} + \frac{r_{n-1}}{r_{n-2}} = q_{n-2} + \frac{1}{\frac{r_{n-2}}{r_{n-1}}} \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}} = q_1 + \frac{1}{\frac{r_{n-1}}{r_n}} \\
\frac{r_{n-1}}{r_n} &= q_n.
\end{aligned}$$

Upon substitution, the value of $\frac{r_1}{r_2}$ from the second equation into the first of the algorithm, we get

$$\frac{u}{v} = q_1 + \frac{1}{q_2 + \frac{1}{r_2/r_3}}.$$

By similar manner, substituting the value of $\frac{r_2}{r_3}$ from the third equation into the previous one, we obtain

$$\frac{u}{v} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{r_3/r_4}}}.$$

Continuing this manner, we obtain

$$\frac{u}{v} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + q_{n-1} + \cfrac{1}{q_n}}}.$$

Therefore $[q_1; q_2, q_3, \ldots, q_n]$. This proves any rational number can be expressed as a finite simple continued fraction. □

In view of foregoing theorem, an interesting question to ask about uniqueness of the representation of a rational number as a finite simple continued fraction. The next theorem will answer the question.

Theorem 11.2.3. *Every rational number can be expressed exactly by two finite simple continued fraction expansions.*

Proof. Let η be a rational number. Then $\exists\, p, q \in \mathbb{Z}$ with $q \neq 0$ and $\gcd(p, q) = 1$ such that $\eta = \frac{p}{q}$. In view of the Theorem 11.2.2 we can say that η can be expressed as $[b_1; b_2, \cdots b_n]$. Then from Euclidean algorithm taking $r_0 = p$ and $r_1 = q$ we have,

$$\begin{aligned}
r_0 &= r_1 b_1 + r_2, & 0 < r_2 < r_1.\\
r_1 &= r_2 b_2 + r_3, & 0 < r_3 < r_2.\\
r_2 &= r_3 b_2 + r_4, & 0 < r_4 < r_3.\\
\vdots &= \vdots\\
r_{n-2} &= r_{n-1} b_{n-1} + r_n, & 0 < r_n < r_{n-1}.\\
r_{n-1} &= r_n b_n.
\end{aligned}$$

The last step of Euclidean algorithm can be written as, $r_{n-1} = (b_n - 1)r_n + r_n$. Then in this case last step will be $r_n = 1 \cdot r_n$. Thus the expression of simple continued fraction will be $[b_1; b_2, \cdots b_n - 1, 1]$. This proves that every rational number can be expressed exactly by two finite simple continued fraction expansions. □

Next, we will talk about the numbers obtained from a finite continued fraction by removing the expression at different stages.

Definition 11.2.2. *The continued fraction $[b_0; b_1, b_3, \ldots, b_k]$ where $k(\in \mathbb{Z}^+) \leq n$, is said to be the k–th convergent of the continued fraction $[b_0; b_1, b_3, \ldots, b_n]$. The k–th convergent of $[b_0; b_1, b_3, \ldots, b_n]$ is denoted by C_k.*

Let $b_0, b_1, \ldots, b_n$ be real numbers, with $b_1, \ldots, b_n$ be positive. Let us define simple fundamental recurrence relations p_k and $q_k (k = 0, 1, 2, 3, \ldots, n)$ as follows:

$$\begin{aligned}
p_0 &= b_0 & q_0 &= 1\\
p_1 &= b_1 b_0 + 1 & q_1 &= b_1\\
p_k &= b_k p_{k-1} + p_{k-2} & q_k &= b_k q_{k-1} + q_{k-2}
\end{aligned}$$

where $k = 2, 3, 4, \ldots, n$. We use this to start with a formulae for the convergents.

Theorem 11.2.4. *The k-th convergent C_k of the finite continued fraction $[b_0; b_1, b_2, b_3, \ldots, b_n]$ has the value $C_k = \frac{p_k}{q_k}$, $0 \leq k \leq n$.*

Proof. We proceed by principles of mathematical induction on k. For $k = 0, 1, 2$, we find

$$\begin{aligned}C_0 &= b_0 = \frac{b_0}{1} = \frac{p_0}{q_0},\\ C_1 &= b_0 + \frac{1}{b_1} = \frac{b_1 b_0 + 1}{b_1} = \frac{p_1}{q_1},\\ C_2 &= b_0 + \frac{1}{b_1 + \frac{1}{b_2}} = \frac{b_2(b_1 b_0 + 1) + b_0}{b_2 b_1 + 1} = \frac{p_2}{q_2}.\end{aligned}$$

Hence the theorem is true for $k = 0, 1, 2$. If possible, let the theorem be true for $k = m$ where $2 \leq m \leq n$. Then

$$C_m = \frac{p_m}{q_m} = \frac{b_m p_{m-1} + p_{m-2}}{b_m q_{m-1} + q_{m-2}}. \tag{11.2.1}$$

Dependence of the real numbers p_{m-1}, p_{m-2}, q_{m-1}, q_{m-2} on the partial quotients $b_1, b_2, b_3, \ldots, b_n$ allow us to replace the real number b_m by $b_m + \frac{1}{b_{m+1}}$ in the (11.2.1), to get

$$\begin{aligned}C_{m+1} &= [b_0; b_1, b_2, b_3, \ldots, b_m, b_{m+1}]\\ &= [b_0; b_1, b_2, b_3, \ldots, b_m, b_m + \frac{1}{b_{m+1}}]\\ &= \frac{(b_m + \frac{1}{b_{m+1}})p_{m-1} + p_{m-2}}{(b_m + \frac{1}{b_{m+1}})q_{m-1} + q_{m-2}}\\ &= \frac{b_{m+1}(b_m p_{m-1} + p_{m-2}) + p_{m-1}}{b_{m+1}(b_m q_{m-1} + q_{m-2}) + q_{m-1}}\\ &= \frac{b_{m+1} p_m + p_{m-1}}{b_{m+1} q_m + q_{m-1}} = \frac{p_{m+1}}{q_{m+1}},\end{aligned}$$

which is true for $k = m + 1$. Hence we are done.

□

Theorem 11.2.5. *If C_k is the k-th convergent of the finite continued fraction $[b_0; b_1, b_2, b_3, \ldots, b_n]$, then for $1 \leq k \leq n$; $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$.*

Proof. We apply mathematical induction on k to prove the theorem. For $k = 1$, we have

$$p_1 q_0 - q_1 p_0 = (b_1 b_0 + 1) \cdot 1 - b_1 b_0 = 1 = (-1)^{1-1}.$$

Assume the theorem is true for $k = m$. Then for $1 \leq m \leq n$, we have

$$p_m q_{m-1} - q_m p_{m-1} = (-1)^{m-1}.$$

Now,

$$\begin{aligned} p_{m+1}q_m - q_{m+1}p_m &= (b_{m+1}p_m + p_{m-1})q_m - (b_{m+1}q_m + q_{m-1})p_m \\ &= -(p_m q_{m-1} - q_m p_{m-1}) \\ &= -(-1)^{m-1} = (-1)^m, \end{aligned}$$

so the theorem prevails for $k = m+1$. This completes the proof by induction. □

An immediate consequence of the foregoing theorem are the following corollaries.

Corollary 11.2.1. *For* $1 \leq k \leq n$, $\gcd(p_k, q_k) = 1$.

Proof. If $d = \gcd(p_k, q_k)$; then by virtue of above theorem, we obtain $d \big| (-1)^{k-1}$. Because $d > 0$, this enables us to conclude $d = 1$. □

Corollary 11.2.2. *For the k-th convergent of the finite simple continued fraction*
$[b_0; b_1, b_2, b_3, \ldots, b_n]$, *the following identities are true.*

1. *for* $1 \leq k \leq n$; $C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$.
2. *for* $2 \leq k \leq n$; $C_k - C_{k-2} = \frac{b_k(-1)^{k-2}}{q_k q_{k-2}}$.

Proof. 1. An immediate consequence of Theorem 11.2.5, yields

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

2. With the aid of $p_k = b_k p_{k-1} + p_{k-2}$ & $q_k = b_k q_{k-1} + q_{k-2}$, we note that

$$\begin{aligned} C_k - C_{k-2} &= \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} \\ &= \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}} \\ &= \frac{(b_k p_{k-1} + p_{k-2})q_{k-2} + p_{k-2}(b_k q_{k-1} + q_{k-2})}{q_k q_{k-2}} \\ &= \frac{b_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1})}{q_k q_{k-2}} \\ &= \frac{b_k(-1)^{k-2}}{q_k q_{k-2}} \quad \text{[by Theorem(11.2.4)].} \end{aligned}$$

This finishes the second identity.

□

With the aid of last two corollaries, we have the following theorem.

Theorem 11.2.6. *Let* C_k *be the* k*-th convergent of the finite simple continued fraction* $[b_0; b_1, b_2, b_3, \ldots, b_n]$*. Then*

$$C_1 > C_3 > C_5 \cdots > \cdots ;$$
$$C_0 < C_2 < C_4 \cdots < \cdots .$$

Also for all $i = 0, 1, 2, 3, 4, \ldots$*; every even-numbered convergent* C_{2i} *is less than every odd-numbered convergent* C_{2i+1}*.*

Proof. As the partial quotients are positive real numbers and $q_j > 0 \; \forall \; j$, replacing k by $k+2$ in Corollary 11.2.2(2), we find that

$$\begin{aligned} C_{k+2} - C_k &= \frac{b_{k+2}(-1)^k}{q_{k+2}q_k} \\ &> 0, \text{ if } k \text{ is even say } k = 2i; \\ &< 0, \text{ if } k \text{ is odd say } k = 2i-1. \end{aligned}$$

Hence

$$C_1 > C_3 > C_5 \cdots > \cdots ; \tag{11.2.2}$$
$$C_0 < C_2 < C_4 \cdots < \cdots . \tag{11.2.3}$$

For the final part, its suffices to show that $C_{2r-1} > C_{2s}$. In view of Theorem 11.2.4, we find that

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

For $k = 2i - 1$, we get

$$C_{2i-1} - C_{2i} = \frac{(-1)^{2i-2}}{q_k q_{k-1}} > 0 \Rightarrow C_{2i-1} > C_{2i}.$$

Hence using (11.2.2) and (11.2.3), we get blending all inequalities together

$$C_{2r-1} > C_{2s+2r-1} > C_{2s+2r} > C_{2s}.$$

□

We conclude this section with the theorem concerning the relation associated with the denominator of the k-th convergent of the finite continued fraction.

Theorem 11.2.7. *If* q_k *is the denominator of the* k*-th convergent* C_k *of the finite continued fraction* $[b_0; b_1, b_2, b_3, \ldots, b_n]$*, then* $q_{k-1} \leq q_k$ *for* $1 \leq k \leq n$*; the strict inequality holds when* $k > 1$*.*

Proof. We will take the help of mathematical induction on k to establish the theorem. For $k = 0$, $q_0 = 1$; $k = 1$, $q_1 = b_1$ and $b_1 \geq 1$. Thus $q_1 \geq q_0$. Assume, the theorem persist for $k = m$ with $1 \leq m < n$. Then, $q_{m-1} \leq q_m$. Now $q_{m+1} = b_{m+1}q_m + q_{m-1} > b_{m+1}q_m \geq 1 \cdot q_m = q_m$. So the inequality prevails for $k = m + 1$. Hence by induction the theorem is established. □

11.3 Worked out Exercises

Problem 11.3.1. *Find the rational number, expressed in lowest terms, represented by each of the following simple continued fractions: (i)*$[3; 7, 15, 1]$ *(ii)*$[2; 1, 2, 1, 1, 4]$

Solution 11.3.1. **(i)** *By virtue of Definition(11.2.1), we obtain*

$$[3; 7, 15, 1] = 3 + \cfrac{1}{7 + \cfrac{1}{15 + 1}} = 3 + \cfrac{1}{7 + \cfrac{1}{16}} = \frac{355}{113}.$$

Remark 11.3.1. $[3; 7, 15, 1]$ *is a good approximation for* π.

(ii)

$$[2; 1, 2, 1, 1, 4] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}} = \frac{87}{32}.$$

Problem 11.3.2. *Find the simple continued fraction, not terminating with the partial quotient of* 1, *of each of the following rational numbers: (i)* $\frac{17}{9}$ *(ii)* $-\frac{746}{830}$.

Solution 11.3.2. *Here we need to apply the proof of Theorem(11.2.2) to find the simple continued fraction expansion. The tool required here is Euclidean algorithm.*

(i) *Applying Euclidean algorithm on* 17 *and* 9 *we have,*

$$17 = 1 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1$$
$$8 = 8 \cdot 1.$$

Thus the sequence of quotients give the continued fraction expansion $[1; 1, 8]$.

(ii) *Again applying Euclidean algorithm on* -746 *and* 830 *we have,*

$$\begin{aligned}-746 &= -1\cdot 830 + 84\\ 830 &= 9\cdot 84 + 74\\ 84 &= 1\cdot 74 + 10\\ 74 &= 7\cdot 10 + 4\\ 10 &= 2\cdot 4 + 2\\ 4 &= 2\cdot 2.\end{aligned}$$

Thus the sequence of quotients give the continued fraction expansion $[-1;9,1,7,2,2]$.

Problem 11.3.3. *Find the convergence of the continued fraction expansion of* $\frac{75}{19}$.

Solution 11.3.3. *We need to find the continued fraction expansion of* $\frac{75}{19}$. *Applying Euclidean algorithm on* 75 *and* 19 *we have,*

$$\begin{aligned}75 &= 3\cdot 19 + 18\\ 19 &= 1\cdot 18 + 1\\ 18 &= 18\cdot 1.\end{aligned}$$

Thus the sequence of quotients generate the continued fraction $[3;1,18]$. *Using the fundamental recurrence relations* p_k *and* $q_k (k = 0,1,2)$, *we compute*

$$\begin{aligned}p_0 &= 3 & q_0 &= 1\\ p_1 &= 1\cdot 3 + 1 = 4 & q_1 &= 1\\ p_2 &= 18\cdot 4 + 3 = 75 & q_2 &= 18\cdot 1 + 1 = 19.\end{aligned}$$

Thus the convergents are $C_0 = \frac{3}{1} = 3$, $C_1 = \frac{4}{1} = 4$ *and* $C_2 = \frac{75}{19}$.

Problem 11.3.4. *Prove that if* $b_0 > 0$ *then* $\frac{p_k}{p_{k-1}} = [b_k; b_{k-1}, \cdots, b_1, b_0]$ *where* $C_{k-1} = \frac{p_{k-1}}{q_{k-1}}$ *and* $C_k = \frac{p_k}{q_k}$, $k \geq 1$ *are successive convergents of the continued fraction* $[b_0; b_1, \cdots b_n]$.

Solution 11.3.4. *Since* C_{k-1} *and* $C_k (k \geq 1)$ *are successive convergents of* $[b_0; b_1, \cdots b_n]$, *therefore fundamental recurrence relations yields* $p_k = b_k p_{k-1} + p_{k-2}$. *Using the relation successively gives,*

$$\frac{p_k}{p_{k-1}} = b_k + \frac{p_{k-2}}{p_{k-1}} = b_k + \frac{1}{\frac{p_{k-1}}{p_{k-2}}}.$$

Again,

$$\frac{p_{k-1}}{p_{k-2}} = b_{k-1} + \frac{1}{\frac{p_{k-2}}{p_{k-3}}}.$$

Thus,

$$\frac{p_k}{p_{k-1}} = b_k + \frac{1}{b_{k-1} + \frac{1}{\frac{p_{k-2}}{p_{k-3}}}}.$$

Proceeding this way, we get

$$\frac{p_2}{p_1} = b_2 + \frac{1}{\frac{p_1}{p_0}}.$$

Since $p_0 = b_0$ *and* $p_1 = b_1 b_0 + 1$ *holds, therefore* $\frac{p_1}{p_0} = b_1 + \frac{1}{b_0}$ *prevails. Piling up all the steps we get,*

$$\frac{p_k}{p_{k-1}} = b_k + \cfrac{1}{b_{k-1} + \cfrac{1}{\ddots + b_1 + \cfrac{1}{b_0}}}.$$

Therefore $\frac{p_k}{p_{k-1}} = [b_k; b_{k-1}, \cdots, b_1, b_0]$.

Problem 11.3.5. *Prove that if the simple continued fraction expression of the rational number* β*,* $\beta > 1$*, is* $[b_0; b_1 \cdots, b_n]$*, then the simple continued fraction expression of* $\frac{1}{\beta}$ *is* $[0; b_0 \cdots, b_n]$*.*

Solution 11.3.5. *Here* β *is a rational number then for any* $r, s \in \mathbb{Z}$ *with* $s \neq 0$ *and* $\gcd(r, s) = 1$ *we can write* $\beta = \frac{r}{s}$*. Since* $\beta > 1$ *then we have* $r > s$*. Also* $[b_0; b_1, \cdots, b_n]$ *is the expression of simple continued fraction* $\frac{r}{s}$*. Again* $\frac{1}{\beta} = \frac{s}{r} < 1$ *implies* $s < r$*. Applying Euclidean algorithm on* s *and* r *we get* $s = 0 \cdot r + s$*,* $r = b_0 \cdot s + b_1$ *and rest of the steps are same as* $\frac{r}{s}$*. Thus the simple continued fraction expression of* $\frac{1}{\beta}$ *is* $[0; b_0 \cdots, b_n]$*.*

The following problem deals with an alternating way of finding the general solution of linear Diophantine equations using simple finite continued fractions.

Problem 11.3.6. *Determine the general solutions of the Diophantine equation* $18x + 5y = 24$*.*

Solution 11.3.6. *Note that* $\gcd(18, 5) = 1$*. The given equation can be re-written as*

$$\frac{18}{1}x + \frac{5}{1}y = \frac{24}{1} \Rightarrow 18x + 5y = 24. \tag{11.3.1}$$

We proceed to solve using two steps. In first step, we will find the particular solution of (11.3.1) when equated to 1 *i.e.* $18x + 5y = 1$ *and thereby in the second step find the general solution of the given equation.*

Step I *We begin by writing* $\frac{18}{5}$*(or if one prefers* $\frac{5}{18}$*) as a simple continued fraction. An appeal to Euclidean algorithm yields*

$$\begin{aligned}18 &= 3\cdot 5+3\\ 5 &= 1\cdot 3+2\\ 3 &= 1\cdot 2+1\\ 2 &= 2\cdot 1,\end{aligned}$$

so that $\frac{18}{5}=[b_0;b_1,b_2,b_3]=[3;1,1,2]=3+\cfrac{1}{1+\frac{1}{1+\frac{1}{2}}}$*. Here using simple fundamental recurrence relations* $p_k,\ q_k$ *for* $k=0,1,2,3$ *we find* $p_0=b_0=3,\ p_1=b_1b_0+1=4,\ p_2=b_2p_1+p_0=7,\ p_3=b_3p_2+p_1=18;\ q_0=1,\ q_1=b_1=1,\ q_2=b_2q_1+q_0=2,\ q_3=b_3q_2+q_1=5$*. The convergents of this simple finite continued fraction are given by,*

$$C_0=\frac{p_0}{q_0}=3,\ C_1=\frac{p_1}{q_1}=4,\ C_2=\frac{p_2}{q_2}=7,\ C_3=\frac{p_3}{q_3}=\frac{18}{5}.$$

In view of Theorem 11.2.5(taking $k=3$*) we obtain* $p_3q_2-q_3p_2=(-1)^{3-1}=1$*, which further yields*

$$18(2)-5(7)=1. \tag{11.3.2}$$

Taking into consideration (11.3.1), when relation (11.3.2) is multiplied by 24 *gives,*

$$18(48)+5(-168)=24.$$

Thus, a particular solution of the Diophantine (11.3.1) is $x_0=48,\ y_0=-168$*.*

Step II *Now by virtue of Theorem 2.7.1, the general solution is given by the equations*

$$x=x_0+bt=48+5t,\ y=y_0-at=-168-18t;\quad t=0,\pm1,\pm2,\ldots.$$

This completes the solution.

11.4 Infinite Continued Fractions

In the present section, we will study infinite continued fractions and establish how to express a real quantity with the help of an infinite continued fraction. We will depict the utilization of the continued fraction representation of a real number to generate rational numbers that are approximations of this real number.

In the subsequent system, we will study infinite continued fractions of quadratic irrationalities.

Let us begin with an infinite sequence of positive integers $a_0, a_1, a_2, \ldots, \ldots,$. To define and to study infinite continued fraction, we need few results from mathematical analysis which we have covered in prerequisites. The following theorem is of fundamental importance, based on the relation between Fibonacci sequence and infinite continued fraction. To know Fibonacci sequence in details, refer to Chapter14(sec 14.1).

Theorem 11.4.1. *For the simple infinite continued fraction* $[b_0; b_1, b_2, b_3, \ldots, b_n]$, *the inequality* $q_k \geq U_k$ $(k = 1, 2, \ldots)$ *holds where* $C_k = \dfrac{p_k}{q_k}$ *is the k-th convergent of the fraction and* U_k *denotes the k-th Fibonacci number(See Chapter* 14*).*

Proof. We establish by mathematical induction. For $k = 1, 2$ we have $q_1 = b_1 \geq 1 = U_1$ and $q_2 = b_2 q_1 + q_0 = b_2 b_1 + b_0 \geq U_2$ respectively. So the result is true for $k = 1, 2$. Let us assume the result be true for $k = m$. Then $q_m \geq U_m$. We are to prove the result for $k = m + 1$. Now

$$\begin{aligned} q_{m+1} &= b_{m+1} q_m + q_{m-1}, \\ &\geq b_{m+1} U_m + U_{m-1}, \\ &\geq U_m + U_{m-1}, \\ &= U_{m+1}, \text{ from the definition of Fibonacci sequence.} \end{aligned}$$

Hence we are done. □

The following theorem define infinite continued fractions as limits of finite continued fractions. The limit η described in the statement of the theorem is called the value of the infinite simple continued fraction $[b_0; b_1, b_2, b_3, \ldots, b_k, \ldots]$.

Theorem 11.4.2. *Let* $\{b_0, b_1, b_2, \ldots\}$ *be an infinite sequence of integers with* b_i, $i = 1, 2, 3, \ldots$ *being positive. Let* $C_k = [b_0; b_1, b_2, b_3, \ldots, b_k]$. *Then* $\lim_{k \to \infty} C_k = \eta$.

Proof. Let $m \in \mathbb{Z}^+$. From Theorem 11.2.5, we see that

$$\begin{aligned} &C_1 > C_3 > C_5 > \cdots > C_{m-1}, \\ &C_0 < C_2 < C_4 \cdots < C_m \end{aligned}$$

and $C_{2j} > C_{2k+1}$ whenever $2j \leq m$ and $2k + 1 < m$. Taking into consideration all possible values of m, we get

$$\begin{aligned} &C_1 > C_3 > C_5 > \cdots > C_{2n-1} > C_{2n+1} > \cdots, \\ &C_0 < C_2 < C_4 \cdots < C_{2n-2} < C_{2n} < \cdots \end{aligned}$$

and $C_{2j} > C_{2k+1} \forall\, j, k \in \mathbb{Z}^+$. Since both the sequences $\{C_1, C_3, C_5, \cdots, C_{2n-1}, C_{2n+1}, \cdots, \}$ and $\{C_0, C_2, C_4 \cdots, C_{2n-2}, C_{2n}, \cdots\}$ are monotone and bounded, therefore they will converge to a definite limit say the sequence $\{C_1, C_3, C_5, \cdots, C_{2n-1}, C_{2n+1}, \cdots, \}$ converges to η_1 and $\{C_0, C_2, C_4 \cdots, C_{2n-2}, C_{2n}, \}\cdot$ converges to η_2 *i.e.*

$$\lim_{k\to\infty} C_{2n+1} = \eta_1, \quad \lim_{k\to\infty} C_{2n} = \eta_2.$$

Claim: $\eta_1 = \eta_2$. Using Corollary 11.2.2(2), we find that

$$C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{(2n+1)-1}}{q_{2n+1}q_{2n}} = \frac{1}{q_{2n+1}q_{2n}}.$$

Also $q_k \geq k \ \ \forall\, k \in \mathbb{Z}^+$ [for details refer to Theorem 11.4.1], yields

$$\frac{1}{q_{2n+1}q_{2n}} < \frac{1}{(2n+1)(2n)}.$$

Hence

$$C_{2n+1} - C_{2n} = \frac{1}{(2n+1)(2n)} \to 0, \ \text{ as } n \to \infty.$$

Hence the sequences $\{C_1, C_3, C_5, \cdots, C_{2n-1}, C_{2n+1}, \cdots, \}$ and $\{C_0, C_2, C_4 \cdots, C_{2n-2}, C_{2n}, \cdots\}$ have the same limit *i.e.* $\eta_1 = \eta_2$. □

Already we have shown that a rational number can be represented as finite simple continued fraction. However, the following theorem shows that the value of any infinite simple continued fraction is irrational.

Theorem 11.4.3. *Let* $\{b_0, b_1, b_2, \ldots\}$ *be an infinite sequence of integers with* b_i, $i = 1, 2, 3, \ldots$ *being positive. Then value of* $[b_0; b_1, b_2, b_3, \ldots, b_k, \ldots]$ *is irrational.*

Proof. Let $\eta = [b_0; b_1, b_2, b_3, \ldots, b_k, \ldots]$ and $C_k = \dfrac{p_k}{q_k} = [b_0; b_1, b_2, b_3, \ldots, b_k]$ denote the k-th convergent of η. For a positive integer n, we have

$$\begin{aligned} &C_{2n} < \eta < C_{2n+1}, \\ &\Rightarrow 0 < \eta - C_{2n} < C_{2n+1} - C_{2n}. \end{aligned} \tag{11.4.1}$$

Applying corollary(11.2.2), we find

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}}. \tag{11.4.2}$$

Feeding (11.4.2) in (11.4.1), gives

$$0 < \eta q_{2n} - p_{2n} < \frac{1}{q_{2n+1}}. \tag{11.4.3}$$

With a view of finding a contradiction, let us assume that η be rational. Then $\exists\, r, s \in \mathbb{Z}$ with $s \neq 0$ and $\gcd(r, s) = 1$ such that $\eta = \dfrac{r}{s}$. Then (11.4.3) yields

$$0 < rq_{2n} - sp_{2n} < \frac{s}{q_{2n+1}}. \tag{11.4.4}$$

It is to be noted that for all positive integers n, $(rq_{2n} - sp_{2n})$ is an integer. However, by virtue of Theorem 11.4.1, $q_{2n+1} > 2n + 1\ \forall\ n \in \mathbb{Z}$. Hence $\exists\ n_0 \in \mathbb{Z}$ such that

$$q_{2n_0+1} > s \Rightarrow \frac{s}{q_{2n_0+1}} < 1,$$

this leads to the contradiction as $(rq_{2n} - sp_{2n})$ cannot lie between 0 and 1. Hence with this finishes the proof.

□

The following theorem shows the uniqueness of the infinite simple continued fraction that represent the same irrational number.

Theorem 11.4.4. *If the two infinite continued fractions* $[b_0; b_1, b_2, b_3, \ldots, b_k, \ldots]$ *and*
$[c_0; c_1, c_2, c_3, \ldots, c_k, \ldots]$ *are equal(or represent the same irrational number), then* $b_n = c_n\ \forall\ n \geq 0$.

Proof. Let $x = \lim_{n\to\infty}[b_0; b_1, b_2, b_3, \ldots, b_k, \ldots]$. Then,

$$C_0 < x < C_1 \Rightarrow b_0 < x < b_0 + \frac{1}{b_1} \Rightarrow b_0 < x < (b_0 + 1) \quad \because\ b_1 \geq 1.$$

Hence $[x] = b_0$. Now, assume $[b_0; b_1, b_2, b_3, \ldots, b_k, \ldots] = x = [c_0; c_1, c_2, c_3, \ldots, c_k, \ldots]$. Then

$$b_0 + \frac{1}{[b_1; b_2, b_3, b_4, \ldots, b_k, \ldots]} = x = c_0 + \frac{1}{[c_1; c_2, c_3, c_4, \ldots, c_k, \ldots]}. \tag{11.4.5}$$

With the help of the reason stated in first paragraph of the proof, we have from (11.4.1)

$$b_0 = [x] = c_0 \Rightarrow [b_1; b_2, b_3, b_4, \ldots, b_k, \ldots] = [c_1; c_2, c_3, c_4, \ldots, c_k, \ldots].$$

By similar reasoning as stated, we next obtain

$$b_1 = [x] = c_1 \Rightarrow [b_2; b_3, b_4, b_5, \ldots, b_k, \ldots] = [c_2; c_3, c_4, c_5, \ldots, c_k, \ldots].$$

Hence the theorem is true for $k = 0, 1$. Now assume $b_k = c_k$ which implies

$$[b_{k+1}; b_{k+2}, b_{k+3}, b_{k+4}, \ldots, \ldots] = [c_{k+1}; c_{k+2}, c_{k+3}, c_{k+4}, \ldots, \ldots].$$

Applying the same argument, we see that

$$b_{k+1} = c_{k+1} \Rightarrow [b_{k+2}; b_{k+3}, b_{k+4}, b_{k+5}, \ldots, \ldots] = [c_{k+2}; c_{k+3}, c_{k+4}, c_{k+5}, \ldots, \ldots].$$

Thus by mathematical induction, our task is complete. ☐

We will now show that every irrational number can be uniquely expressed by an infinite simple continued fraction.

Theorem 11.4.5. *Let* $\eta = \eta_0$ *be irrational and define the sequence* $\{b_0, b_1, b_2, \ldots\}$ *recursively by*

$$b_k = [\eta_k],\ \eta_{k+1} = \frac{1}{\eta_k - b_k},\ k = 0, 1, 2, 3, \ldots\ldots.$$

Then $\eta = \lim_{k\to\infty} C_k$*, where* $C_k = [b_0; b_1, b_2, b_3, \ldots, b_k]$.

Proof. From the given recursive definition, we find b_k is an integer for every k. We are to prove η_k is irrational for every k. We will take the help of mathematical induction on k to fulfill our claim. For $k = 0$, $\eta_0 = \eta$ is irrational. Let for $k = m$, η_m be irrational number. Now,

$$\eta_{m+1} = \frac{1}{\eta_m - b_m} \Rightarrow \eta_m = b_m + \frac{1}{\eta_{m+1}}. \tag{11.4.6}$$

If η_{m+1} is rational, then η_m is also so, which contradicts the induction hypothesis. Hence η_{m+1} is irrational number. Now as η_m is irrational and b_k is an integer, we know that $\eta_m \neq b_m$ and

$$\begin{aligned} & b_m < \eta_m < b_m + 1(\text{Why!}), \\ \Rightarrow\ & 0 < \eta_m - b_m < 1, \\ \Rightarrow\ & \eta_{m+1} = \frac{1}{\eta_m + b_m} > 1, \\ \Rightarrow\ & b_{m+1} = [\eta_{m+1}] \geq 1, \end{aligned}$$

for $k = 0, 1, 2, 3, \ldots$. This shows $b_i; i = 1, 2, \ldots$ are all positive integers. On repetitive use of (11.4.2), we find

$$\begin{aligned}\eta = \eta_0 &= b_0 + \frac{1}{\eta_1} = [b_0; \eta_1]\\ &= b_0 + \frac{1}{\frac{1}{b_1 + \frac{1}{\eta_2}}} = [b_0; b_1, \eta_2]\\ &= \vdots\\ &= \vdots\\ &= b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots + b_k + \cfrac{1}{\eta_{k+1}}}}} = [b_0; b_1, b_2, \ldots, b_k, \eta_{k+1}].\end{aligned}$$

Now our next claim is $[b_0; b_1, b_2, \ldots, b_k, \eta_{k+1}] \to \eta$ as $k \to \infty$. By virtue of Theorem 11.2.3, we have

$$\begin{aligned}\eta &= [b_0; b_1, b_2, \ldots, b_k, \eta_{k+1}]\\ &= \frac{\eta_{k+1} p_k + p_{k+1}}{\eta_{k+1} q_k + q_{k-1}},\end{aligned}$$

where $C_j = \dfrac{p_j}{q_j}$ is the jth convergent of $[b_0; b_1, b_2, \ldots, b_k, \ldots]$. Hence

$$\begin{aligned}\eta - C_k &= \frac{\eta_{k+1} p_k + p_{k+1}}{\eta_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k},\\ &= \frac{-(p_k q_{k-1} - p_{k-1} q_k)}{(\eta_{k+1} q_k + q_{k-1}) q_k}\\ &= \frac{(-1)^k}{(\eta_{k+1} q_k + q_{k-1}) q_k} \text{[By Theorem(11.2.5)]}.\end{aligned}$$

Since, $\eta_{k+1} q_k + q_{k-1} > b_{k+1} q_k + q_{k-1} = q_{k+1}$, therefore,

$$|\eta - C_k| < \frac{1}{q_k q_{k+1}} \to 0, \quad \text{as } k \to \infty.$$

Hence the proof. □

In our next example will illustrate the fact behind Theorem 11.4.5.

Example 11.4.1. *Consider* $\eta_0 = \sqrt{7}$. *Then* $b_0 = [\sqrt{7}] = 2$ *and* $\eta_1 = \dfrac{1}{\eta_0 - b_0} = \dfrac{1}{\sqrt{7} - 2} = \dfrac{\sqrt{7} + 2}{2}$. *This gives* $b_1 = \left[\dfrac{\sqrt{7} + 2}{2}\right] = 2$. *By similar way, we find*

$\eta_2 = \dfrac{1}{\eta_1 - b_1} = \dfrac{2(\sqrt{7}+2)}{3}$. Continuing this manner, we get $b_2 = 3, b_3 = 10$ and $b_4 = 3$. Thus the expression for $\sqrt{7}$ is $[2; 2, 3, 10, 3, \cdots]$.

The next theorem will illustrate the fact that the convergents of the simple infinite continued fraction of η are the best rational approximations to it.

Theorem 11.4.6. *Let η be an irrational number and let $\frac{p_j}{q_j}$, $j = 1, 2, 3, \ldots$ be the convergents of the infinite simple continued fraction of η. If $r, s \in \mathbb{Z}$ with $s > 0$ such that $|s\eta - r| < |q_k\eta - p_k|$, then $s \geq q_{k+1}$.*

Proof. Given that $|s\eta - r| < |q_k\eta - p_k|$; to the contrary assume that $1 \leq s \leq q_{k+1}$. To begin with consider the system of simultaneous equations

$$p_k x + p_{k+1} y = r \tag{11.4.7}$$

$$q_k x + q_{k+1} y = s. \tag{11.4.8}$$

Now, (11.4.7) $\times\, q_k$ $-$ (11.4.8) $\times\, p_k$ gives

$$(p_{k+1}q_k - p_k q_{k+1})y = rq_k - sp_k.$$

Taking into consideration Theorem(11.2.5), we find

$$y = (-1)^k(rq_k - sp_k).$$

By similar reasoning; (11.4.8) $\times\, p_{k+1}$ $-$ (11.4.7) $\times\, q_{k+1}$ yields

$$x = (-1)^k(sp_{k+1} - rq_{k+1}).$$

Claim: $x \neq 0,\ y \neq 0$. If $x = 0$, then $sp_{k+1} = rq_{k+1}$. Since $\gcd(p_{k+1}, q_{k+1}) = 1$, therefore $q_{k+1}|s \Rightarrow q_{k+1} \leq s$, contradicts our assumption. If $y = 0$, then $r = p_k x,\ s = q_k x$[by (11.4.7) and (11.4.8)] implies

$$|s\eta - r| = |x||q_k\eta - p_k| \geq |q_k\eta - p_k|,\ [\because\ |x| \geq 1].$$

This steers contradiction to the stated condition. Hence $x \neq 0,\ y \neq 0$. Finally we note that x and y are of opposite signs. Consider $y < 0$. Since $q_k x = s - q_{k+1}y$ [refer to (11.4.7)], we have $x > 0$ because $q_k x > 0$ and $q_k > 0$. When $y > 0$ we see that $q_k x < 0$ as $s < q_{k+1}$. So $x < 0$. Since $\frac{p_k}{q_k} < \eta < \frac{p_{k+1}}{q_{k+1}}$, we find $q_k\eta - p_k$ and $q_{k+1}\eta - p_{k+1}$ are of opposite sign. From (11.4.7) and (11.4.8), we obtain

$$\begin{aligned} |s\eta - r| &= |(q_k x + q_{k+1}y)\eta - (p_k x + p_{k+1}y)| \\ &= |x(q_k\eta - p_k) + y(q_{k+1}\eta - p_{k+1})|. \end{aligned}$$

Combining the conclusions of the previous two paragraphs, we get $x(q_k\eta - p_k)$ and $y(q_{k+1}\eta - p_{k+1})$ have the same sign, so

$$\begin{aligned}|s\eta - r| &= |x||\,|x(q_k\eta - p_k)| + |y||\,|x(q_{k+1}\eta - p_{k+1})| \\ &\geq |x||x(q_k\eta - p_k)| \\ &\geq |x(q_k\eta - p_k)|, \because\ |x| \geq 1.\end{aligned}$$

Finally, this contradicts our given fact. Hence $1 \leq s \leq q_{k+1}$ fails. Consequently, the proof is complete. □

The following well-known theorem leads to the fact that the convergents of the infinite simple continued fraction of an irrational number are good approximations to η.

Theorem 11.4.7. *Dirichlet's Theorem on Diophantine Approximation: If η is an irrational number, then there are infinitely many rational numbers $\frac{r}{s}$ such that $|\eta - \frac{r}{s}| < \frac{1}{2s^2}$.*

Proof. Let $\frac{r_k}{s_k}$ be the k-th convergent of the continued fraction of η. Following the proof of Theorem 11.4.5, we get

$$|\eta - \frac{r_k}{s_k}| < \frac{1}{s_k s_{k+1}} < \frac{1}{s_k^2}\ [\because,\ s_k < s_{k+1}].$$

Consequently, $\frac{r_k}{s_k}$(convergents of η) $k = 1, 2, 3, \ldots$ are infinitely many rational numbers satisfying the conditions stated in the theorem. □

The concluding theorem of this section focusses on the fact that any rational number which approximates very closely an irrational number must be a convergent of the infinite simple continued fraction of this number.

Theorem 11.4.8. *If η is an irrational number and $\frac{u}{v}$ is a rational number with $v > 0$ such that $|\eta - \frac{u}{v}| < \frac{1}{2v^2}$, then $\frac{u}{v}$ is a convergent of the simple continued fraction representation of η.*

Proof. Assume that $\frac{u}{v}$ is not a convergent of the simple infinite continued fraction expansion of η. Then $\exists$ successive convergents $\frac{p_k}{q_k}$ and $\frac{p_{k+1}}{q_{k+1}}$ such that $q_k \leq s < q_{k+1}$. From Theorem 11.4.6, we see that

$$\begin{aligned}|q_k\eta - p_k| \leq |v\eta - u| = v\left|\eta - \frac{u}{v}\right| < \frac{1}{2v}. \\ \Rightarrow \left|\eta - \frac{p_k}{q_k}\right| < \frac{1}{2vq_k},\ \text{[Dividing by } q_k].\end{aligned}$$

Since $|vp_k - uq_k| \geq 1$(we know that $vp_k - uq_k$ is non-zero integer as $\frac{u}{v} \neq \frac{p_k}{q_k}$), it follows that

$$\begin{aligned}\frac{1}{vq_k} \leq \frac{|vp_k - uq_k|}{vq_k} &= \left|\frac{p_k}{q_k} - \frac{u}{v}\right| \\ &\leq \left|\eta - \frac{p_k}{q_k}\right| + \left|\eta - \frac{u}{v}\right| \\ &< \frac{1}{2vq_k} + \frac{1}{2v^2}.\end{aligned}$$

(where we have used the triangle inequality to obtain the second inequality above). Hence

$$\frac{1}{2vq_k} < \frac{1}{2v^2} \Rightarrow 2vq_k > 2v^2 \Rightarrow q_k > v,$$

contradicting our assumption. □

11.5 Worked out Exercises

Problem 11.5.1. *Find the simple infinite continued fraction of* $\frac{1+\sqrt{5}}{2}$.

Solution 11.5.1. *Let us consider* $\eta_0 = \frac{1+\sqrt{5}}{2}$. *Then* $a_0 = \left[\frac{1+\sqrt{5}}{2}\right] = 1$. *Applying Theorem 11.4.5 we obtain* $\eta_1 = \frac{1}{\eta_0 - a_0} = \frac{2}{\sqrt{5}-1} = \frac{\sqrt{5}+1}{2} = \eta_0$. *This gives* $\frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, 1, \ldots, \ldots]$.

Problem 11.5.2. *Prove that the first four partial quotients of the simple infinite continued fraction of* $\frac{e-1}{e+1}$ *are* $0, 2, 6, 10$.

Solution 11.5.2. *Suppose* $\eta_0 = \frac{e-1}{e+1}$. *Then* $b_0 = \left[\frac{e-1}{e+1}\right] = 0$. *In view of Theorem(11.4.5), we get* $\eta_1 = \frac{1}{\eta_0 - b_0} = \frac{e+1}{e-1}$. *Then,* $b_1 = [\eta_1] = \left[\frac{e+1}{e-1}\right] = 2$. *Again,* $\eta_2 = \frac{1}{\eta_1 - b_1} = \frac{1}{\frac{e+1}{e-1} - 2} = -\frac{e-1}{e-3}$. *Consequently,* $b_2 = [\eta_2] = \left[-\frac{e-1}{e-3}\right] = 6$. *By similar manner,* $\eta_3 = \frac{1}{\eta_2 - b_2} = \frac{1}{\eta_2 - 6} = -\frac{e-3}{7e-19}$, $b_3 = [\eta_3 = 10]$. *Thus the first four partial quotients of the simple infinite continued fractions of* $\frac{e-1}{e+1}$ *are* $b_0 = 0, b_1 = 2, b_2 = 6, b_3 = 10$.

Problem 11.5.3. *Let* γ *and* δ *be two real numbers. Then* γ *is equivalent to* δ *if* $\exists$ *integers* a, b, c *and* d *satisfying* $ad - bc = \pm 1$ *and* $\gamma = \frac{a\delta+b}{c\delta+d}$. *Prove that if* γ *is equivalent to* δ, *then* δ *is also equivalent to* γ.

Solution 11.5.3. *Since γ is equivalent to δ then we can write $\gamma = \frac{a\delta+b}{c\delta+d}$ for some integers a, b, c and d with $ad - bc = \pm 1$. Now,*

$$\begin{aligned} \gamma c\delta + \gamma d &= a\delta + b \\ \gamma c\delta - a\delta &= b - \gamma d \\ \delta(\gamma c - a) &= b - \gamma d \\ \delta &= \frac{\gamma d - b}{\gamma c - a}. \end{aligned}$$

Here we have $(-a)d - (-b)c = bc - ad = \pm 1$. This results in δ is equivalent to γ.

Problem 11.5.4. *Prove that the i-th convergent of the simple infinite continued fraction of $\frac{1}{\eta}$ is the reciprocal of the $(i-1)$-th convergent of the simple infinite continued fraction of η, where $\eta(> 1)$ is an irrational quantity.*

Solution 11.5.4. *Let the simple infinite continued fraction of η be $[b_0; b_1, b_2, \ldots]$. Then $\dfrac{1}{\eta} = \dfrac{1}{[b_0; b_1, b_2, \ldots]} = [0; b_0, b_1, b_2, \ldots]$[refer to Problem(11.3.5)]. Now the i-th convergent of $\dfrac{1}{\eta}$ is*

$[0; b_0, b_1, b_2, \ldots, b_{i-1}]$. Therefore $[0; b_0, b_1, b_2, \ldots, b_{i-1}] = 0 + \dfrac{1}{a_0 + \frac{1}{B}}$ where $B = [b_1; b_2, b_3, b_4, \ldots, b_{i-1}] = \dfrac{1}{b_0 + \frac{1}{B}} = \dfrac{1}{[b_0; b_1, b_2, \ldots b_{i-1}]}$. Here $[b_0; b_1, b_2, \ldots b_{i-1}]$ is the $(i-1)$-th convergent of η. This proves the statement.

Problem 11.5.5. *Let η be an irrational number with simple infinite continued fraction expansion $[b_0; b_1, b_2, \ldots]$. Prove that the simple continued fraction of $-\eta$ is $[-b_0 - 1; 1, b_1 - 1, b_2, b_3, \ldots]$ if $b_1 > 1$ and $[-b_0 - 1; b_2 + 1, b_3, \ldots]$ if $b_1 = 1$.*

Solution 11.5.5. *Here η is an irrational number with simple infinite continued fraction expansion $[b_0; b_1, b_2, \ldots]$. Let us take $B = [b_2; b_3, b_3, b_4, \ldots]$. If $b_1 > 1$, then we have*

$$\begin{aligned} &[b_0; b_1, b_2, \ldots] + [-b_0 - 1; 1, b_1 - 1, b_2, b_3, \ldots] \\ &= b_0 + \frac{1}{b_1 + \frac{1}{B}} + (-b_0 - 1) + \frac{1}{1 + \frac{1}{(b_1 - 1)} + \frac{1}{B}} \\ &= b_0 + \frac{B}{b_1 B + 1} - b_0 - 1 + \frac{1}{1 + \frac{B}{b_1 B - B + 1}} \\ &= \frac{B}{b_1 B + 1} - 1 + \frac{b_1 B - B + 1}{b_1 B + 1} \\ &= 0. \end{aligned}$$

If $b_1 = 1$, *then we need to consider* $B = [b_3; b_4, b_5, b_6, \dots,]$. *Thus we have,*

$$\begin{aligned}
&[b_0; b_1, b_2, \dots] + [-b_0 - 1; b_2 + 1, b_2, b_3, \dots] \\
&= b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \frac{1}{B}}} + (-b_0 - 1) + \frac{1}{(b_2 + 1) + \frac{1}{B}} \\
&= b_0 + \frac{1}{1 + \frac{B}{b_2 B + 1}} - 1 + \frac{B}{b_2 B + B + 1} \\
&= \frac{b_2 B + 1}{b_2 B + 1 + B} - 1 + \frac{B}{b_2 B + B + 1} \\
&= 0.
\end{aligned}$$

11.6 Periodic Fractions

In continuation with example(11.4.1), we find $b_5 = b_1$, $b_6 = b_2$ and so on. The process iterates repeatedly, which makes the sequence of partial quotients periodic. So this example motivates us to study the notion of periodic infinite simple continued fractions. In the present section, we will show that the necessary and sufficient condition for an infinite continued fraction to be periodic is that the real number represented by the continued fraction is a quadratic irrational. So let us begin with a definition.

Definition 11.6.1. *An infinite simple continued fraction* $[b_0; b_1, b_2, \dots, \dots]$ *is said to be periodic if* $\exists$ *positive integers* N *and* k *such that* $b_n = b_{n+k}$ *for all positive integers* n *with* $n \geq N$. *Symbolically, periodic fraction are represented by* $[b_0; b_1, b_2, b_{N-1}, \overline{b_N, b_{N+1}, \dots, b_{N+k-1}}]$. *It means periodic infinite simple continued fraction are expressed as*

$$[b_0; b_1, b_2, b_{N-1}, b_N, b_{N+1}, \dots, b_{N+k-1}, b_N, b_{N+1}, \dots].$$

To characterize irrational numbers with periodic infinite simple continued fractions, we need the following definition.

Definition 11.6.2. *Quadratic Irrationalities: A real number* η *is said to be a quadratic irrational if* η *is irrational and if* η *is a root of a quadratic equation with integral coefficients given by* $Ax^2 + Bx + C = 0$, *where* A, B, C *are integers.*

Before we proceed with important results, let us start with an important theorem about quadratic irrationalities.

Theorem 11.6.1. *A real number* η *is said to be a quadratic irrational if and only if* $\exists$ *integers* a, b, c *such that* b *is not a perfect square and satisfies* $\eta = \dfrac{a + \sqrt{b}}{c}$ *where* $b > 0$ *and* $c \neq 0$.

Proof. Let us assume the real number η to be a quadratic irrational. Then η is irrational and also $\exists$ integers $A,\ B,\ C$ such that η is a root of the quadratic equation $Ax^2+Bx+C=0$. Hence $\eta=\dfrac{-B\pm\sqrt{B^2-4AC}}{2A}$ with $A\neq 0$. Since η is real, therefore $B^2-4AC>0$. Also B^2-4AC can not be a perfect square[Why!]. Considering the values of a,b,c as follows:

$$a=b,\ b=B^2-4AC,\ C=-2A \text{ or } a=-B,\ b=B^2-4AC,\ c=2A,$$

we obtain $\eta=\dfrac{a+\sqrt{b}}{c}$ where $b>0$ and $c\neq 0$.

For the converse part, assume that for some integers $a,\ b,\ c$ with $b>0$ and $c\neq 0$ such that b is not a perfect square and $\eta=\dfrac{a+\sqrt{b}}{c}$. Then η is irrational. Also,

$$\eta=\frac{a+\sqrt{b}}{c}\Rightarrow\sqrt{b}=c\eta-a.$$

Squaring, we get

$$b=(c\eta-a)^2\Rightarrow c^2\eta^2-2ac\eta+(a^2-b)=0.$$

This implies $A=c^2,\ B=-2ac,\ C=a^2-b$. Hence η is a quadratic irrational. This completes the proof. □

An immediate consequence of Theorem 11.6.1 leads to a corollary of importance.

Corollary 11.6.1. *Let η be a quadratic irrational. Then $\exists$ integers a,b and c with $c\neq 0,\ b(>0)$ is not a perfect square and $c\big|(b-a^2)$.*

Proof. We have $\eta=\dfrac{a+\sqrt{b}}{c}$. Then multiplying numerator and denominator by $|c|$ we obtain $\eta=\dfrac{a|c|+\sqrt{bc^2}}{c|c|}$. Here $a|c|,\ c|c|$ & bc^2 are all integers with $c|c|\neq 0$ as $c\neq 0$. Also $bc^2>0$ as $b>0$ and bc^2 is not a perfect square as b is not so. Hence comparing $\eta=\dfrac{a|c|+\sqrt{bc^2}}{c|c|}$ with $\eta=\dfrac{a+\sqrt{b}}{c}$ gives

$$b-a^2=bc^2-a^2c^2=c^2(b-a^2)\Rightarrow c\big|(b-a^2).$$

This completes the proof. □

The following theorem can be applied when periodic simple continued fractions represent quadratic irrationalities.

Theorem 11.6.2. *If η be a quadratic irrational and if $r,\ s,\ t,\ u$ are integers, then $\dfrac{r\eta+s}{t\eta+u}$ is either rational or a quadratic irrational.*

Proof. Since η is a quadratic irrational, the last lemma ensures the existence of integers $a,\ b,\ c$ such that b is not a perfect square and satisfies $\eta = \dfrac{a+\sqrt{b}}{c}$ with $b > 0$ and $c \neq 0$. On simplification, we get

$$\begin{aligned}\frac{r\eta+s}{t\eta+u} &= \frac{(ar+cs)+r\sqrt{b}}{(at+cu)+t\sqrt{b}}\\ &= \frac{[(ar+cs)(at+cu)-rtb]+[r(at+cu)-t(ar+cs)]\sqrt{b}}{(at+cu)^2-t^2b}.\end{aligned}$$

Hence if the coefficients of $\sqrt{b}$ vanishes, then $\dfrac{r\eta+s}{t\eta+u}$ becomes rational, otherwise quadratic irrational. □

For our future discussions of simple continued fractions of quadratic irrationalities, we will need the notion of the conjugate of a quadratic irrationality, whose definition is as follows.

Definition 11.6.3. *Let* $\eta = \dfrac{a+\sqrt{b}}{c}$, *where* $b > 0$ *and* $c \neq 0$, *be a quadratic irrational. Then the conjugate of* η, *denoted by,* $\bar{\eta}$ *is defined by* $\bar{\eta} = \dfrac{a-\sqrt{b}}{c}$.

Theorem 11.6.3. *If the quadratic irrational* η *is a root of the polynomial* $Ax^2 + Bx + C = 0$, *where* A, B, C *are integers, then the other root of the polynomial is* $\bar{\eta}$, *the conjugate of* η.

Proof. Obvious. □

The following theorem deals with few properties involving quadratic irrationalities.

Theorem 11.6.4. *If* $\eta_1 = \dfrac{a_1+b_1\sqrt{d}}{c_1}$ *and* $\eta_2 = \dfrac{a_2+b_2\sqrt{d}}{c_2}$ *are quadratic irrationals, then the following statements are true:*

1. $\overline{(\eta_1+\eta_2)} = \bar{\eta}_1 + \bar{\eta}_2$.
2. $\overline{(\eta_1-\eta_2)} = \bar{\eta}_1 - \bar{\eta}_2$.
3. $\overline{\eta_1\eta_2} = \overline{\eta_1}\,\overline{\eta_2}$.
4. $\overline{\left(\dfrac{\eta_1}{\eta_2}\right)} = \dfrac{\overline{\eta_1}}{\overline{\eta_2}}$.

Proof. Left to the reader. □

The central theorem about periodic simple continued fractions is commonly known as Lagrange's theorem. Although, Euler proved a part of the theorem. In 1737 Euler proved that a periodic infinite simple continued fraction represents a quadratic irrationality. Later in 1770, Joseph-Louis Lagrange showed that a quadratic irrationality has a periodic continued fraction.

To prove the converse part of Lagrange's theorem, that the simple continued fraction of a quadratic irrationality is periodic, we need the following theorem for obtaining the continued fraction of a quadratic irrational.

Theorem 11.6.5. *Let η be a quadratic irrational. Then $\exists$ integers A_0, B_0 & d such that $\eta = \dfrac{A_0 + \sqrt{d}}{B_0}$ with $B_0 \neq 0$, $d > 0$ and d is not a perfect square with $B_0 \big| (d - A_0^2)$. Define recursively, $\eta_k = \dfrac{A_k + \sqrt{d}}{B_k}$, $b_k = [\eta_k]$, $b_{k+1} = b_k B_k - A_k$ & $B_{k+1} = \dfrac{d - A_{k+1}^2}{B_k}$, $k = 0, 1, 2, 3, \ldots$. Then $\eta = [b_0; b_1, b_2, b_3, \ldots]$.*

Proof. Taking aid of mathematical induction, we will prove that A_k, $B_k \in \mathbb{Z}$ with $B_k \neq 0$ and $B_k \big| (d - A_k^2)$ for $k = 0, 1, 2, 3, 4, \ldots$. For $k = 0$, the assertion follows from the given condition of the theorem. Assume the statement is true for $k = m$. Then A_m, $B_m \in \mathbb{Z}$ with $B_m \neq 0$ and $B_m \big| (d - A_m^2)$ holds. We are to show that the statement is true for $k = m + 1$. Now $A_{m+1} = b_m B_m - A_m \in \mathbb{Z}$. Further,

$$\begin{aligned} B_{m+1} &= \frac{d - A_{m+1}^2}{B_m} = \frac{1}{B_m}\{d - (b_m B_m - A_m)^2\} \\ &= \frac{1}{B_m}\{d - b_m^2 B_m^2 - A_m^2 + 2b_m A_m B_m\} \\ &= \frac{d - A_m^2}{B_m} + (2b_m A_m - b_m^2 B_m) \\ &= \frac{d - A_m^2}{B_m} + b_m(2A_m - b_m B_m). \end{aligned} \tag{11.6.1}$$

By induction hypothesis, $B_m \big| (d - A_m^2)$. Hence by (11.6.1) $B_{m+1} \in \mathbb{Z}$. Since d is not a perfect square, we get $d \neq A_m^2 \Rightarrow B_{m+1} \neq 0$. Since $B_m = \dfrac{d - A_{m+1}^2}{B_{m+1}}$ therefore, $B_{m+1} \big| (d - A_{m+1}^2)$. For the concluding part of the theorem, its suffices to show that $\eta_{k+1} = \dfrac{1}{\eta_k - b_k}$ for $k = 0, 1, 2, 3, \ldots$. Now

$$\begin{aligned}
\eta_k - b_k &= \frac{A_k + \sqrt{d}}{B_k} - b_k \\
&= \frac{\sqrt{d} - (b_k B_k - A_k)}{B_k} \\
&= \frac{\sqrt{d} - A_{k+1}}{B_k} = \frac{d - A_{k+1}^2}{B_k(\sqrt{d} + A_{k+1})} = \frac{B_{k+1}}{\sqrt{d} + A_{k+1}} = \frac{1}{\eta_{k+1}}.
\end{aligned}$$

Hence from the foregoing equation the desired result follows. □

Theorem 11.6.6. *Lagrange's Theorem: Any periodic simple infinite continued fraction of an irrational number is a quadratic irrational, and vice-versa.*

Remark 11.6.1. *It is to be noted that this theorem is different from Lagrange's theorem on polynomial congruences discussed in Chapter 8.*

Proof. Let η be the irrational number and the simple infinite continued fraction of it be periodic. We are to prove η is quadratic irrational. Then

$$\eta = [b_0; b_1, b_2, b_3, \ldots, b_{N-1}, \overline{b_N, b_{N+1}, \ldots, b_{N+k}}].$$

Let

$$\begin{aligned}
\beta &= [\overline{b_N; b_{N+1}, \ldots, b_{N+k-1}, b_{N+k}}] \\
&= [b_N; b_{N+1}, \ldots, b_{N+k-1}, b_{N+k}, \beta].
\end{aligned}$$

Then from Theorem 11.2.3 it follows that

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}, \tag{11.6.2}$$

where

$$\begin{aligned}
\frac{p_k}{q_k} &= \lim_{k \to \infty} [b_N; b_{N+1}, \ldots, b_{N+k-1}, b_{N+k}] \\
\frac{p_{k-1}}{q_{k-1}} &= \lim_{k \to \infty} [b_N; b_{N+1}, \ldots, b_{N+k-1}, b_{N+k}].
\end{aligned}$$

Here we note that β is irrational[Why!] and in view of (11.6.2), we find

$$q_k \beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0.$$

Consequently, β is quadratic irrational. Further,

$$\eta = [b_0; b_1, b_2, b_3, \ldots, b_{N-1}, \beta].$$

Then $\eta = \dfrac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}}$ where $\dfrac{p_{N-1}}{q_{N-1}}$ and $\dfrac{p_{N-2}}{q_{N-2}}$ are convergent of $[b_0; b_1, b_2, b_3, \ldots, b_{N-1}]$. Taking into consideration Theorem 11.6.2, η is quadratic irrational as β is so. Hence we are done.

For the converse part, assume η to be a quadratic irrational. Then by Theorem 11.6.5 $\eta = \dfrac{A_0 + \sqrt{d}}{B_0}$. Furthermore, we have $\eta = [b_0; b_1, b_2, b_3, \ldots,]$ where $\eta_k = \dfrac{A_k + \sqrt{d}}{B_k}$, $b_k = [\eta_k]$, $A_{k+1} = b_k B_k - A_{k+1}$, $B_{k+1} = \dfrac{d - A_{k+1}^2}{B_{k+1}}$, $k = 0, 1, 2, 3, 4, \ldots$.

Since $\eta = [b_0; b_1, b_2, b_3, \ldots, \eta_k]$ therefore, by virtue of Theorem 11.2.3 we find $\eta = \dfrac{A_{k-1}\eta_k + A_{k-2}}{B_{k-1}\eta_k + B_{k-2}}$. Taking conjugates on both sides, we obtain

$$\overline{\eta} = \frac{A_{k-1}\overline{\eta_k} + A_{k-2}}{B_{k-1}\overline{\eta_k} + B_{k-2}} \text{ [refer to Theorem 11.6.4].} \tag{11.6.3}$$

Solving for $\overline{\eta_k}$ yields,

$$\overline{\eta_k} = -\frac{B_{k-2}}{B_{k-1}} \left[\frac{\overline{\eta} - \frac{A_{k-2}}{B_{k-2}}}{\overline{\eta} - \frac{A_{k-1}}{B_{k-1}}} \right].$$

Since

$$\eta = \lim_{k \to \infty} \frac{A_{k-2}}{B_{k-2}} = \lim_{k \to \infty} \frac{A_{k-1}}{B_{k-1}}$$

therefore,

$$\lim_{k \to \infty} \frac{\overline{\eta} - \frac{A_{k-2}}{B_{k-2}}}{\overline{\eta} - \frac{A_{k-1}}{B_{k-1}}} = 1.$$

Hence by definition of convergence $\exists\, N \in \mathbb{Z}$ such that $\overline{\eta_k} < 0 \;\forall\; k \geq N$. Since $\eta_k > 0$ for $k \geq 1$, we get

$$\eta_k - \overline{\eta_k} = \frac{A_k + \sqrt{d}}{B_k} - \frac{A_k - \sqrt{d}}{B_k} = \frac{2\sqrt{d}}{B_k} > 0.$$

So $B_k > 0 \;\forall\; k \geq N$. Since $B_k B_{k+1} = d - A_{k+1}^2$, we see that for $k \geq N$

$$0 \leq B_k \leq B_k B_{k+1} = d - A_{k+1}^2 \leq d. \tag{11.6.4}$$

Also $k \geq n$ yields $A_{k+1}^2 \leq d = A_{k+1}^2 - B_k B_{k+1}$, which gives

$$-\sqrt{d} < A_{k+1} < \sqrt{d} \tag{11.6.5}$$

For $k \geq N$, the inequalities (11.6.4) and (11.6.5) generates finite number of values for A_k, B_k. Since there are infinitely many integers k for $k \geq N$ therefore,

$\exists$ two integers i and j such that $A_i = A_j$ and $B_i = B_j$ for $i < j$. Hence from the defining relation for η_k, we see that $\eta_i = \eta_j$. In consequence, we find $b_i = b_j$, $b_{i+1} = b_{j+1}$, $b_{i+2} = b_{j+2}$ and so on. Thus,

$$\begin{aligned}\eta &= [b_0; b_1, b_2, b_3, \ldots, b_{i-1}, b_i, b_{i+1}, \ldots, b_{j-1}, b_i, b_{i+1}, \ldots, b_{j-1}, \ldots]\\ &= [b_0; b_1, b_2, b_3, \ldots, b_{i-1}, \overline{b_j, b_{i+1}, \ldots, b_{j-1}}].\end{aligned}$$

This completes the proof. □

11.7 Worked out Exercises

Problem 11.7.1. *Find the simple continued fraction of* $\frac{14+\sqrt{37}}{3}$.

Solution 11.7.1. *Note that* $\eta = \frac{14+\sqrt{37}}{3}$. *Taking help of Theorem 11.6.5, set* $A_0 = 14$, $B_0 = 3$, *and* $d = 37$. *Then* $b_0 = [\frac{14+\sqrt{37}}{3}] = 6$. *Using the value* $A_0 = 14$, $B_0 = 3$ *we find* $A_1 = b_0 B_0 - A_0 = 4$ *and* $B_1 = \frac{d-A_1^2}{B_0} = 7$. *Blending* A_1 *and* B_1 *yields* $\eta_1 = \frac{4+\sqrt{37}}{7}$. *Hence* $b_1 = [\eta_1] = 1$. *Again taking* $A_1 = 4$, $B_1 = 7$ *we get,* $A_2 = b_1 B_1 - A_1 = 3$, $B_2 = 4$ *and* $\eta_2 = \frac{3+\sqrt{37}}{4}$. *Thus* $b_2 = [\eta_2] = 2$. *In similar manner, we get* $A_3 = 5$, $B_3 = 3$ *and combining these two we obtain* $b_3 = [\eta_3] = 3$. *Continuing this way, we see that* $b_4 = b_1$, $b_5 = b_2$, $b_6 = b_3$ *and so on. Thus the continued fraction expansion of* $\frac{14+\sqrt{37}}{3}$ *is* $[6; \overline{1, 2, 3}]$.

Problem 11.7.2. *Find the simple continued fraction of* $\sqrt{203}$.

Solution 11.7.2. *Note that* $\eta = \sqrt{203}$. *Taking help of Theorem 11.6.5, we write* $\eta_0 = \sqrt{203}$. *We set* $A_0 = 0$, $B_0 = 1$, $d = 203$. *Then* $b_0 = [\sqrt{203}] = 14$. *Using the value* $A_0 = 0$, $B_0 = 1$, *we find* $A_1 = b_0 B_0 - A_0 = 14$ *and* $B_1 = \frac{d-A_1^2}{B_0} = 7$. *Taking* A_1 *and* B_1 *together, we have* $\eta_1 = \frac{14+\sqrt{203}}{7}$. *Hence* $b_1 = [\eta_1] = 4$. *Again considering* $A_1 = 14$, $B_1 = 7$ *we obtain* $A_2 = b_1 B_1 - A_1 = 14$, $B_2 = 1$ *and* $\eta_2 = \frac{14+\sqrt{203}}{1}$. *Hence* $b_2 = [\eta_2] = 28$. *In similar manner we can find* $A_3 = 14$, $B_3 = 7$ *and taking these two value together* $b_3 = [\eta_3] = 4 = b_1$. *Continuing this way, we see that* $b_4 = b_2$ *and so on. Thus the continued fraction expansion of* $\sqrt{203}$ *is* $[14; \overline{4, 28}]$.

Problem 11.7.3. *Find the quadratic irrationality of* $[\overline{1; 2, 3}]$.

Solution 11.7.3. *Let* $x = [\overline{1; 2, 3}]$. *Then from Theorem 11.6.6, we can say that* x *is a quadratic irrational. Note that* x *can be written as*

$$x = 1 + \cfrac{1}{2 + \frac{1}{3+\frac{1}{x}}} = \frac{10x+3}{7x+2} \Rightarrow 7x^2 - 8x - 3 = 0.$$

Since x *is positive, therefore on solving we obtain* $x = \dfrac{4+\sqrt{37}}{7}$.

Problem 11.7.4. *Find the period length of the simple continued fraction of $\sqrt{d^2+1}$, where d is a non negative integer.*

Solution 11.7.4. *Here $\eta_0 = d^2+1$ implies $b_0 = [\eta_0] = d$. Now we can find $A_1 = b_0B_0 - A_0 = d$ and $B_1 = (d^2+1) - d^2 = 1$. Therefore $\eta_1 = d + \sqrt{d^2+1}$ and $b_1 = [\eta_1] = 2d$. Similarly we have $A_2 = b_1B_1 - A_1 = d$ and $B_2 = 1$. It follows that $\eta_2 = d + \sqrt{d^2+1}$ and $b_2 = [\eta_2] = 2d = b_1$. Therefore the expression for $\sqrt{d^2+1}$ is $[d; \overline{2d}]$ and it is of period length one.*

Problem 11.7.5. *For an integer m with $m \geq 3$, find the simple continued fraction for $\sqrt{m^2-2}$. Hence find $\sqrt{47}$.*

Solution 11.7.5. *Note that $m-1 < \sqrt{m^2-1} < m$. Now we have $\eta_0 = \sqrt{m^2-1} = \sqrt{(m-1)^2}+2m-3$. Therefore $b_0 = [\eta_0] = m-1$. Here $A_0 = 0$ and $B_0 = 1$. Then $A_1 = (m-1)\cdot 1 - 0 = m-1$, $B_1 = \dfrac{m^2-2-(m-1)^2}{1} = 2m-3$. Thus we get, $\dfrac{m-1+\sqrt{m^2-2}}{2m-3}$. Since $m-1 < \sqrt{m^2-2} < m$, therefore*

$$\frac{(m-1)-(m-1)}{2m-3} < \frac{(m-1)+\sqrt{m^2-2}}{2m-3} < \frac{(m-1)+m}{2m-3}.$$

This yields, $b_1 = [\eta_1] = 1$. Similarly, we get $A_2 = b_1B_1 - A_1 = m-2$, $B_2 = \dfrac{A_2+\sqrt{m^2-2}}{B_2} = \dfrac{(m-2)+\sqrt{m^2-2}}{2}$. Therefore $b_2 = [\eta_2] = m-2$;$A_3 = b_2B_2 - A_2 = (m-2)\cdot 2 - (m-2) = m-2$, $B_3 = \frac{(m^2-2)^2-A_3^2}{B_2} = 2m-3$. Therefore $\eta_3 = \dfrac{A_3+\sqrt{m^2-2}}{B_3} = 2m-3$. Hence $b_3 = [\eta_3] = 1$(by using the above inequality);$A_5 = b_4B_4 - B_4 = A_1$, $B_5 = 2m-3 = B_1$. Thus the simple continued fraction for $\sqrt{m^2-2}$ is $[(m-1); \overline{1, m-2, 1, 2m-2}]$. Hence using this, we obtain $\sqrt{47} = \sqrt{49-2} = \sqrt{7^2-2}$. Thus the simple continued fraction for $\sqrt{47}$ is $[6; 1, 5, 1, 12]$.

11.8 Exercises:

1. Compute the rational number in lowest terms, represented by each of the following simple finite continued fractions: (i)$[1; 2, 1, 2]$ (ii)$[1; 1, 1, 1, 1]$.
2. Compute the simple finite continued fraction, not terminating with the partial denominators of 1, of each of the following rational numbers: (i) $\dfrac{310}{99}$ (ii) $-\dfrac{943}{1001}$.
3. Compute the convergence of the expansion of the following continued fractions : (i) $\frac{19}{29}$ (ii)$\frac{32}{17}$.

4. Prove: If $b_0 > 0$, then $\frac{q_k}{q_{k-1}} = [b_k; b_{k-1}, \cdots, b_2, b_1]$ where $C_{k-1} = \frac{p_{k-1}}{q_{k-1}}$ and $C_k = \frac{p_k}{q_k}$, $k \geq 1$ are successive convergents of the continued fraction $[b_0; b_1, \cdots b_n]$.

5. Using continued fraction, determine the general solutions of the Diophantine equation $364x + 227y = 1$.

6. Find the simple infinite continued fractions of the followings: (i) $\sqrt{2}$ (ii)$\sqrt{5}$.

7. Determine the first four partial quotients of the following simple infinite continued fractions : (i) 2π (ii)$\frac{e^2 - 1}{e^2 + 1}$.

8. Prove that a real number r is equivalent to itself.

9. Prove that if r_1, r_2 and r_3 are real numbers such that r_1 and r_2 are equivalent and r_2 and r_3 are equivalent, then r_1 and r_3 are equivalent.

10. Find the simple continued fractions of the followings: (i) $\sqrt{37}$ (ii)$\sqrt{209}$ (iii)$1 + \sqrt{2}$ (iv)$\frac{13 - \sqrt{2}}{7}$.

11. Determine the quadratic irrationality of the followings: (i) $[5; \overline{10}]$ (ii)$[1; 2, \overline{3}]$ (iii)$[\overline{2; 1, 5}]$.

12. For an integer m with $m \geq 2$, prove that the simple continued fraction of $\sqrt{m^2 - m}$ is $[m - 1; \overline{2, 2m - 2}]$.

13. Prove that for any positive integer m the simple continued fraction of $\sqrt{m^2 + 2}$ is $[m; \overline{m, 2m}]$. Hence find $\sqrt{51}$.

14. Show that for any positive odd integer $m(> 3)$ the simple continued fraction of $\sqrt{m^2 - 4}$ is $[m - 1; \overline{1, \frac{m-3}{2}, 2, \frac{m-3}{2}, 1, 2m - 2}]$.

15. Find the period length of the simple continued fraction of $\sqrt{m^2 + n}$, where m and n are integers, $n > 1$ and $n | 2m$.

12

Few Non-Linear Diophantine Equations

"I count Maxwell and Einstein, Eddington and Dirac, among "real" mathematicians. The great modern achievements of applied mathematics have been in relativity and quantum mechanics, and these subjects are at present at any rate, almost as "useless" as the theory of numbers."

– Godfrey Harold Hardy

12.1 Introduction

Diophantine equations are those equations restricted to only integral solutions. In chapter2 (Section 2.7), we have studied only linear Diophantine equations. There we discussed how the integral solutions can be calculated. But what about non-linear Diophantine equations? Unlike linear Diophantine equations, in general there is no method for solving all non-linear Diophantine equations. However, few non-linear Diophantine equations as well as their certain families can be solved using many results. The present chapter addresses few non-linear Diophantine equations which are solvable. In the first section, we consider the Diophantine equations of the form $x^2 + y^2 = z^2$, where x, y, z forms the length of the side of the right triangle. A triple (x, y, z) of integers that solve this equation is called Pythagorean Triples. Subsequently, we will focus on the famous Diophantine equation $x^n + y^n = z^n$ where $n > 2$. Fermat stated that there $\nexists$ any solutions of this Diophantine equation, a statement commonly known as

Fermat's Last theorem. The proof of the statement was one of the greatest challenges of mathematics. After a long span of time, in 1995 English mathematician Sir Andrew John Wiles gave the first proof of the statement. The proof is beyond the scope of the book.

12.2 Pythagorean Triples

Definition 12.2.1. *A Pythagorean triple(also known as Pythagorean triangle) is a set of three integers* a, b, c *satisfying* $a^2 + b^2 = c^2$ *and is said to be primitive if* $\gcd(a, b, c) = 1$*. For instance if we take* $5, 12, 13$ *where* $5^2 + 12^2 = 13^2$*, then* $5, 12, 13$ *are said to form Pythagorean triple. Similarly,* $3, 4, 5$ *and* $6, 8, 10$ *are also so. Here the first two triples* $5, 12, 13$ *and* $3, 4, 5$ *are primitive but the last one is not as* $\gcd(6, 8, 10) = 2$*.*

For a Pythagorean triple $6, 8, 10$, if we divide each element of the triple by 2, then the triple becomes $3, 4, 5$ which is both primitive and Pythagorean. In general, for a Pythagorean triple a, b, c where $\gcd(a, b, c) = d$, $\exists$ integers a', b', c' where $a = da',\ b = db',\ c = dc'$ with $\gcd(a', b', c') = 1$. This triple a', b', c' also form a Pythagorean triple as

$$a'^2 + b'^2 = \frac{a^2 + b^2}{d^2} = \frac{c^2}{d^2} = c'^2.$$

Hence a', b', c' forms a primitive Pythagorean triple. Here the key idea is very simple, all Pythagorean triples can be found by forming integral multiples of primitive Pythagorean triples.

Next, the following two lemmas will pave the way for finding all primitive Pythagorean triples.

Lemma 12.2.1. *If* a, b, c *is a primitive Pythagorean triple, then they are mutually prime to each other.*

Proof. Its suffices to show that, for any primitive Pythagorean triple a, b, c; $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$. To begin with, consider $\gcd(a, b) > 1$. Then $\exists$ a prime p such that $p \big| \gcd(a, b)$. This implies $p|a$ and $p|b$. Hence $p|(a^2 + b^2)$. As $p|c^2$ then $p|c$, otherwise for some integer k and r with $0 < r < k$;

$$c = pk + r \Rightarrow c^2 = p(p^2k^2 + 2kr) + r^2.$$

This contradicts $p|c^2$. So $p|a,\ p|b,\ p|c$ altogether gives $\gcd(a, b, c) > 1$. This is impossible as a, b, c is a primitive Pythagorean triple. Therefore $\gcd(a, b) = 1$. Similarly, $\gcd(a, c) = \gcd(b, c) = 1$. ☐

Taking advantage of the last lemma, we will proceed for the next lemma. But before that, let us state and prove a simple but significant result related to congruence.

Result 12.2.1. *Square of any integer is either congruent to* 0 *or* 1 *modulo* 4.

Proof. Consider $n \in \mathbb{Z}$. If n is even, then $n = 2k$ for some integer k. On squaring we obtain

$$n^2 = 4k^2 \equiv 0(\mod 4).$$

If n is odd, then $n = 2k' + 1$ for some integer k'. Proceeding as above, we obtain

$$n^2 = 4k'^2 + 4k' + 1 \equiv 1(\mod 4).$$

□

Lemma 12.2.2. *Let a, b, c be three positive integers with* $\gcd(a, b) = 1$ *and* $ab = c^2$. *Then* $\exists\, m, n \in \mathbb{Z}$ *such that* $a = m^2$ *and* $b = n^2$.

Proof. For $a = 1$ or $b = 1$, the lemma is obvious. So let us begin by taking $a > 1$ and $b > 1$. Let

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},\ b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s},$$

be the prime factorizations of a and b respectively. Since $\gcd(a, b) = 1$, therefore $p_x' s$ are same as q_y for $x = 1, 2, 3, \ldots, r$ and $y = 1, 2, 3, \ldots, s$. Again

$$ab = c^2 \Rightarrow p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s} = z_1^{2t_1} z_2^{2t_2} \cdots z_l^{2t_l},$$

where $c = z_1^{2t_1} z_2^{2t_2} \cdots z_l^{2t_l}$ be the prime factorization of c. Now we appeal to Fundamental theorem of Arithmetic to obtain the fact that the prime powers on both sides of the equation will be same. So each p_x is same as z_ω for some $\omega = 1, 2, 3, \ldots, l$ with coordinated exponents $k_x = 2t_\omega$. In similar manner, each q_y is same as z_ω with coordinated exponents $j_y = 2t_\omega$. Blending them, yields $a = m^2$ and $b = n^2$ where $m = p_1^{\frac{k_1}{2}} p_2^{\frac{k_2}{2}} \cdots p_r^{\frac{k_r}{2}}$ and $n = q_1^{\frac{j_1}{2}} q_2^{\frac{j_2}{2}} \cdots q_s^{\frac{j_s}{2}}$. Hence we are done. □

Making use of Lemma 12.2.2, we come up to the characterization of Pythagorean triple.

Theorem 12.2.1. *The positive integers a, b, c with $2 \big| b$ form a primitive Pythagorean triple if and only if there exist integers x and y such that*

$$a = x^2 - y^2,\ b = 2xy,\ c = x^2 + y^2$$

where $x > y$ and both cannot be even or odd simultaneously.

Proof. Let a, b, c be a Pythagorean triple. Because b is even, both a and c are odd. Then $a+c$ and $a-c$ are even, which implies $\exists$ integers $r, s (> 0)$ such that $r = \dfrac{a+c}{2}$ and $s = \dfrac{a-c}{2}$. Also,

$$a^2 + b^2 = c^2 \Rightarrow b^2 = c^2 - a^2 \Rightarrow \left(\frac{b}{2}\right)^2 = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right).$$

Here we note that $\gcd(r, s) = 1$. If not, let $\gcd(r, s) = d$. Then $d|r$, $d|s$ together yields $d\big|(r+s) = a$ and $d\big|(r-s) = c$. Thus $d\big|\gcd(a, c) = 1$, which is impossible. In view of Lemma 12.2.2, $\exists$ integers x, y such that $r = x^2$ and $s = y^2$. Hence a, b, c can be written in terms of x, y as

$$a = r - s = x^2 - y^2 \tag{12.2.1}$$

$$b = \sqrt{4rs} = 2xy \tag{12.2.2}$$

$$c = r + s = x^2 + y^2. \tag{12.2.3}$$

Claim: $\gcd(x, y) = 1$. To the contrary, assume $d' = \gcd(x, y)$. Then $d'|x$ and $d'|y$. This renders $d'\big|a = x^2 - y^2$, $d'\big|b = 2xy$, $d'\big|x^2 + y^2$; which contradicts $\gcd(a, b, c) = 1$. Putting all discussions into together, we conclude $\gcd(x, y) = 1$. The final touch is to consider both x, y to be odd integers. An appeal to (12.2.1) bring forth all the integers a, b, c to be even. This results in contradiction to $\gcd(a, b, c) = 1$. Since $\gcd(x, y) = 1$, so x, y cannot be even or odd simultaneously.

For the converse part, let us begin with

$$\begin{aligned} a^2 + b^2 &= (x^2 - y^2)^2 + 4x^2y^2 \\ &= (x^2 + y^2)^2 = c^2, \end{aligned}$$

which shows a, b, c form a Pythagorean triple. For the primitive part, assume $\gcd(a, b, c) = d (> 1)$. Then $\exists$ a prime p such that $p\big|\gcd(a, b, c)$. Here $p \neq 2$, otherwise a becomes even which is not possible as $a = x^2 - y^2$ and both x, y cannot be even or odd simultaneously. Also, $p|a$ and $p|c$ together gives $p\big|(a+c) = 2x^2$ and $p\big|(a-c) = 2y^2$. Hence $p|x$, $p|y$ contradicts $\gcd(x, y) = 1$. Thus our assumption, $\gcd(a, b, c) = d$ fails. Hence $\gcd(a, b, c) = 1$ and a, b, c forms a Pythagorean triple. □

Let us run through a specific example to exemplify the theorem lucidly.

Example 12.2.1. *Consider* $x = 7$ *and* $y = 4$. *Here* $\gcd(7, 4) = 1$. *Following* *the above theorem, we get*

$$\begin{aligned} a &= x^2 - y^2 = 33 \\ b &= 2xy = 56 \\ c &= x^2 + y^2 = 65, \end{aligned}$$

is a primitive Pythagorean triple.

Taking advantage of the previous theorem, our last theorem leads to an interesting geometric fact related to Pythagorean triple (Pythagorean triangle).

Theorem 12.2.2. *The radius of the inscribed circle of a Pythagorean triple (Pythagorean triangle) is always an integer.*

Proof. Geometrically, Pythagorean triple is a right angle triangle whose sides are of integral length.

Let r denotes the radius of the inscribed circle. Here the area of the triangle is $ab = r(a+b+c)$. Now, $a^2 + b^2 = c^2$ and as the triple is not primitive then for any integer $k > 0$

$$a = k(x^2 - y^2),\ b = 2kxy,\ c = k(x^2 + y^2),$$

where x, y are positive integers. On substitution, we obtain $r = k(x-y)y$. Hence the proof is established. ☐

12.3 Worked out Exercises

Problem 12.3.1. *Find all primitive Pythagorean triples* a, b, c *with* $b = 40$.

Solution 12.3.1. *From Theorem 12.2.1 the form of Pythagorean triple we get,*

$$a = x^2 - y^2,\ b = 2xy,\ c = x^2 + y^2.$$

Since $b = 40$ *and* $\gcd(x, y) = 1$ *with* $2 \nmid (x+y)$ *(Why!), therefore we have either* $x = 5,\ y = 4$ *or* $x = 20,\ y = 1$*. So the triples are* $9, 40, 41$ *and* $399, 40, 401$.

Problem 12.3.2. *Prove that if* a, b, c *is a Pythagorean triple, then exactly one of* a, b *and* c *is divisible by* 4.

Solution 12.3.2. *If* a, b, c *is a Pythagorean triple, then*

$$a = x^2 - y^2,\ b = 2xy,\ c = x^2 + y^2.$$

where either x *is even or* y*. Then* xy *must be even. This shows that* $2|xy \Rightarrow 4|2xy = b$.

This proves our assertion.

Problem 12.3.3. *Let* $x_1 = 3,\ y_1 = 4,\ z_1 = 5$ *and* x_n, y_n, z_n *for* $n = 2, 3, 4, \ldots$ *be defined recursively by,*

$$\begin{aligned} x_{n+1} &= 3x_n + 2z_n + 1 \\ y_{n+1} &= 3x_n + 2z_n + 2 \\ z_{n+1} &= 4x_n + 3z_n + 2. \end{aligned}$$

Show that x_n, y_n, z_n *is a Pythagorean triple.*

Solution 12.3.3. *In anticipation of mathematical induction, the basis step is* $x_1^2 + y_1^2 = 3^2 + 4^2 = 5^2 = z_1^2$*. This shows that* x_1, y_1, z_1 *is a Pythagorean triple. Let us assume that* x_n, y_n, z_n *is a Pythagorean triple. Now,*

$$\begin{aligned} x_{n+1}^2 + y_{n+1}^2 &= (3x_n + 2z_n + 1)^2 + (3x_n + 2z_n + 2)^2 \\ &= 18x_n^2 + 8z_n^2 + 24x_nz_n + 18x_n + 12z_n + 5 \\ &= (16x_n^2 + 9z_n^2 + 24x_nz_n + 16x_n + 12z_n + 4) + (2x_n^2 - z_n^2 + 2x_n + 1) \\ &= z_{n+1}^2 + \{(x_n^2 + 2x_n + 1) + (x_n^2 - z_n^2)\} \\ &= z_{n+1}^2 + \{(x_n + 1)^2 - y_n^2\} \\ &= z_{n+1}^2\ [\because x_n + 1 = y_n]. \end{aligned}$$

So the result is true for all integer $n \geq 1$*.*

Problem 12.3.4. *Find all solutions in positive integers of the Diophantine equation* $x^2 + 2y^2 = z^2$*.*

Solution 12.3.4. *Here* $2y^2 = z^2 - x^2 = (z + x)(z - x)$*. If we consider* x *as even number, then* z *is also even. This implies* $\frac{x+z}{2}$ *and* $\frac{z-x}{2}$ *both are integers.*

If $\gcd(\frac{z-x}{2}, z + x) = 1$*, then by Lemma 12.2.2 there exists integers* m *and* n *such that* $\frac{z-x}{2} = m^2$ *and* $z + x = n^2$*. Thus solving we get,*

$$x = \frac{m^2 - 2n^2}{2},\ y = mn,\ z = \frac{n^2 + 2m^2}{2}.$$

Similarly, if we consider $\gcd(\dfrac{z + x}{2}, z - x) = 1$ *then by the same argument we get*

$$x = \frac{2m^2 - n^2}{2},\ y = mn,\ z = \frac{2m^2 + n^2}{2}.$$

Problem 12.3.5. *Prove that if* a, b, c *is a primitive Pythagorean triple in which* b *and* c *are consecutive positive integers, then* $a = 2y + 1, b = 2y(y + 1), c = 2y(y + 1) + 1$ *for some* $y > 0$*.*

Solution 12.3.5. *Here the Pythagorean triple are such that* $b+1=c$. *Now* $a=x^2-y^2,\ b=2xy,\ c=x^2+y^2$. *This implies*

$$\begin{aligned}2xy+1&=x^2+y^2\\(x-y)^2&=1\\x&=y+1.\end{aligned}$$

This shows that the Pythagorean triple is of the form

$$a=(y+1)^2-y^2=2y+1,\ b=2y(y+1),\ c=2y(y+1)+1.$$

Problem 12.3.6. *Show that there exists infinitely many primitive Pythagorean triple* a,b,c *whose even member* b *is a perfect square.*

Solution 12.3.6. *Let us consider a triple as* $a=n^4-4,\ b=4n^2,\ c=n^4+4$. *It is clear that* $\gcd(a,b,c)=1$. *Now we are to verify these triples* a,b,c *as a Pythagorean triple. Here*

$$\begin{aligned}a^2+b^2&=(n^4-4)^2+16n^4\\&=n^8-8n^4+16+16n^4\\&=(n^4+4)^2=c^2.\end{aligned}$$

As n *is arbitrary integer, then there are infinite number of Pythagorean triple of these type.*

Problem 12.3.7. *Find all Pythagorean triples containing the integer* 12.

Solution 12.3.7. *Note that we need to find all primitive triples containing a divisor of* 12*;* $2,3,4,6,12$. *The triple is of the form* $a=x^2-y^2,\ b=2xy,\ c=x^2+y^2$, *and* $\gcd(x,y)=1$. *Now here* b *is even. Thus*

if $b=2xy=2$, *then* $x=y=1$ *and* $a=0$ *which is not possible.*

If $b=2xy=4$, *then* $x=2,y=1$ *which shows* $a=3,\ c=5$.

If $b=2xy=6$, *then* $x=3,y=1$ *and they are not of opposite parity.*

If $b=2xy=12$, *then either* $x=6,y=1$ *which shows* $a=35,c=37$ *or* $x=3,y=2$ *showing* $a=5,c=13$.

Here $c\neq 3$ *as* 9 *can not be written as sum of two squares. If* $a=3=x^2-y^2=(x+y)(x-y)$, *then* $x=2,\ y=1,\ b=4$, *and* $c=5$. *Therefore the Pythagorean triples containing* 12 *are;* $(9,12,15),(35,12,37),(5,12,13)$ *and* $(16,12,20)$.

Problem 12.3.8. *For an arbitrary positive integer* n, *show that there exists a Pythagorean triangle the radius of whose inscribed circle is* n.

Solution 12.3.8. *Let n be an arbitrary positive integer and r be the radius of the circle inscribed in the triangle having sides m', n', p'. Then $r = \dfrac{m'+n'-p'}{2}$. Here if $m' = 2n+1,\ n' = 2n^2+2n,\ p' = 2n^2+2n+1,$ then $m'^2 + n'^2 = p'^2$ forms a Pythagorean triangle and $r = n$.*

12.4 Fermat's Last Theorem

In the foregoing section, we dealt with the solvability of Diophantine equations of the form $a^2+b^2 = c^2$ where a, b, c form a primitive Pythagorean triple. Consider the question, whether the solvability of the last equation can be preserved if we change the exponents of a, b, c by an integer greater than 2? Fermat has stated a conjecture, commonly known to be Fermat's Last theorem, that it is impossible to write a cube as a sum of two cubes and in general any exponent as a sum of two similar exponents. Many Mathematicians had given futile efforts to prove the assertion.

Statement 12.4.1. *Fermat's Last Theorem: The Diophantine equation $a^n + b^n = c^n$ has no solution in non-zero integers a, b, c where n is an integer ≥ 3.*

Our future discussions will be based on a special case when $n = 4$, although it is the time for all positive integers m with $3 \leq m \leq 12500$. The technique used for the proof is known as 'method of infinite descent' introduced by Fermat. By virtue of the method we can establish that the Diophantine equation $a^4+b^4 = c^2$ has no solution. This leads to the stronger aspect than showing Fermat's Last theorem for $n = 4$, since any solution of $a^4 + b^4 = c^4 = (c^2)^2$ gives a solution of $a^4 + b^4 = c^2$.

Theorem 12.4.1. *The Diophantine equation $a^4 + b^4 = c^2$ has no non-zero solutions for the positive integers a, b, c.*

Proof. To the contrary, suppose a_0, b_0, c_0 be a positive solutions of $a^4 + b^4 = c^2$. Here we note that $\gcd(a_0, b_0) = 1$, for if $\gcd(a_0, b_0) \neq 1$ then $\gcd(a_0, b_0) = d$(say). This implies $a_0 = da_1,\ b_0 = db_2$ for some positive integers a_1 and b_1 with $\gcd(a_1, b_1) = 1$. As a_0, b_0, c_0 satisfies $a^4 + b^4 = c^2$, we can write $a_0^4 + b_0^4 = c_0^2$ or $(a_0^2)^2 + (b_0^2)^2 = (c_0)^2$ so that a_0^2, b_0^2, c_0 is a primitive Pythagorean triple. In view of Theorem 12.2.1, we find

$$\begin{aligned} a_0^2 &= s^2 - t^2 \\ b_0^2 &= 2st \\ c_0 &= s^2 + t^2. \end{aligned}$$

where s, t are positive integer with $s > t$ and both s and t can not be even or odd simultaneously. Then $a_0^2 + t^2 = s^2$. Consider t be even. Then s is odd. It follows for some positive integer r, $t = 2r$. Now $t_0^2 = 2st = 4sr$ or $\left(\frac{b_0}{2}^2 = sr\right)$. Again, since $\gcd(s, t) = 1$, then $\gcd(s, r) = 1$. taking into consideration Lemma 12.2.2, we find $s = c_1^2$, $r = y_1^2$ for some positive integer c_1 and y_1. Now $\gcd(s, t) = 1 \Rightarrow \gcd(s, a_0, t) = 1$. This yields s, a_0, t to be Pythagorean triple. Now, by virtue of Theorem 12.2.1 we get

$$a_0^2 = u^2 - v^2,\ t = 2uv,\ s = u^2 + v^2,$$

where $\gcd(u, v) = 1$, $u > v > 0$. Then $uv = \frac{t}{2} = r = y_1^2$. Employing Lemma 12.2.2, produces $u = a_1^2$ and $v = b_1^2$. Substitute these values in $u^2 + v^2 = s$ to obtain $a_1^4 + b_1^4 = c_1^2$. Here, $c_1 < c_1^4 = s^2 < s^2 + t^2 = c_0$. Continuing this manner infinite number of times, we obtain monotone decreasing sequence $\{c_0, c_1, c_2, c_3, \ldots, \ldots, \ldots\}$. Since $\exists$ only a finite number of positive integers less than c_0, then this leads to a contradiction, which makes our assumption wrong. Thus the Diophantine equation $a^4 + b^4 = c^2$ has no non-zero solutions for the positive integers a, b, c. □

Taking advantage of the theorem, we have the following corollary.

Corollary 12.4.1. *The equation* $a^4 + b^4 = c^4$ *has no solution in positive integers.*

Theorem 12.4.2. *The area of a Pythagorean triangle can never be equal to a perfect square.*

Proof. Consider a Pythagorean triangle with sides a, b, c satisfies $a^2 + b^2 = c^2$. The area of the triangle is $\frac{1}{2}ab$. Let the area be a perfect square. Then for some integer x, we have $\frac{1}{2}ab = x^2$. It follows $2ab = 4x^2$. On addition and subtraction with $a^2 + b^2 = c^2$, we obtain

$$(a + b)^2 = c^2 + 4x^2,\ (a - b)^2 = c^2 - 4x^2.$$

Therefore

$$(a^2 - b^2)^2 = c^4 - (4x^2)^2 = c^4 - (2x)^4.$$

In view of last remark, it follows that $\nexists$ any solution of the last equation, which makes our task complete. □

12.5 Worked out Exercises

Problem 12.5.1. *Show that the equation* $x^p + y^p = z^p$ *has no solutions in non-zero integers,* p *being an odd prime.*

Solution 12.5.1. *Let* $n(\geq 3) \in \mathbb{Z}$. *By Fermat's theorem,* $x^n + y^n = z^n$ *has no solution for integers* x, y, z. *If* n *has an odd prime factor then* $n = pk$ *for some* $k \in \mathbb{Z}^+$. *Then we have,* $(x^k)^p + (y^k)^p = (z^k)^p$. *Consequently,* $x^p + y^p = z^p$ *has no solution in non-zero integers. If* n *has no odd factor then* n *is some power of* 2. *Since* $n > 2$, $4|n \Rightarrow n = 4k'$ *for some* $k' \in \mathbb{Z}^+$. *Thus* $(x^{k'})^4 + (y^{k'})^4 = (z^{k'})^4$ *has no solution.*

Problem 12.5.2. *Show that the Diophantine equation* $x^4 - y^4 = z^2$ *has no solutions in non-zero integers.*

Solution 12.5.2. *Rewriting the Diophantine equation* $x^4 - y^4 = z^2$ *as* $x^4 = z^2 + y^4$, *we get by Theorem 12.2.1*

$$z = 2st,\ y^2 = s^2 - t^2,\ x^2 = s^2 + t^2.$$

Therefore $s^4 - t^4 = x^2y^2 = (xy)^2$ *is a smaller solution as* $0 < s < \sqrt{s^2 + t^2} = x$. *Now,*

$$y^2 = 2st,\ z = s^2 - t^2,\ x^2 = s^2 + t^2,$$

where s *is even and* t *being odd. Since* $\gcd(s, t) = \gcd(2s, t) = 1$, *in view of Lemma 12.2.2 we obtain* $2s = \omega^2$, $t = v^2$. *As* ω *is even so it takes the form* $\omega = 2u$, $s = 2u^2$. *Hence* $x^2 = 4u^4 + v^4$. *Also, this implies that* $2u^2, v^2, x$ *forms a primitive Pythagorean triple. Again an appeal to Theorem 12.2.1 for* $a > b > 0$, *we find* $2u^2 = 2ab$, $v^2 = a^2 - b^2$, $x = a^2 + b^2$ *where* $\gcd(a, b) = 1$. *Thus* $u^2 = ab$ *ensures* $a = c^2$, $b = d^2$*[refer to Lemma 12.2.2]. Hence* $v^2 = a^2 - b^2 = c^4 - d^4$, *which is also a smaller solution [Why!]. In consequence, we arrive at a contradiction in both the cases. Hence we are done.*

Problem 12.5.3. *Use Fermat's Little theorem to verify that if* p *is prime and* $x^p + y^p = z^p$ *holds, then* $p\big|(x + y - z)$.

Solution 12.5.3. *By Fermat's Little Theorem, for any two integers* x, y *we have* $x^p \equiv x (\bmod\ p)$ *and* $y^p \equiv y (\bmod\ p)$. *Then from equation* $x^p + y^p = z^p$ *we have*

$$\begin{aligned}
& x^p + y^p \equiv (x + y)(\bmod\ p) \\
\Rightarrow\ & z^p \equiv (x + y)(\bmod\ p) \\
\Rightarrow\ & z \equiv (x + y)(\bmod\ p),\ \textit{as}\ z^p \equiv z(\bmod\ p) \\
\Rightarrow\ & p\big|(x + y - z).
\end{aligned}$$

Problem 12.5.4. *Show that the Diophantine equation* $x^2 + y^2 = z^3$ *has infinitely integral solutions by showing that for each positive integer* k,

$$x = 3k^2 - 1,\ y = k(k^2 - 3),\ z = k^2 + 1,$$

form a solution.

Solution 12.5.4. *Here*

$$\begin{aligned} x^2+y^2 &= (3k^2-1)^2[k(k^2-3)]^2 \\ &= 9k^4-6k^2+1+k^2(k^4-6k^2+9) \\ &= (k^2+1)^3 = z^3. \end{aligned}$$

Thus the Diophantine equation $x^2+y^2=z^3$ *has infinitely integral solutions.*

Problem 12.5.5. *In a Pythagorean triple* x, y, z *prove that not more than one of* x, y *or* z *can be a perfect square.*

Solution 12.5.5. *To the contrary, let us begin with the Pythagorean triple* x, y, z *such that more than one of* x, y *or* z *can be a perfect square. As* x, y, z *forms Pythagorean triple, it follows* $x^2+y^2=z^2$*. Now, two cases may arise:*

Case I *If* $x=m^2,\ y=n^2$ *for* $\forall\ m,n\in\mathbb{Z}$*, then* $x^4+y^4=z^2$ *has a solution. But from Theorem 12.4.1, no solution exists of this form. Hence the assumption is not possible.*

Case II *If* $x=m^2,\ y=z^2$ *for* $\forall\ m,n\in\mathbb{Z}$*, then* $x^4+y^4=z^2$ *has a solution, which is not possible by Problem 12.5.2. So our assumption fails for both the cases.*

Problem 12.5.6. *Verify that the only solution in relatively prime positive integers of the equation* $x^4-y^4=2z^2$ *is* $x=y=z=1$.

Solution 12.5.6. *The given Diophantine equation is*

$$x^4-y^4=2z^2. \tag{12.5.1}$$

Squaring both sides of (12.5.1), we get

$$\begin{aligned} (x^4-y^4)^2 &= 4z^4 \\ \text{or } (x^4-y^4)^2+4x^4y^4 &= 4z^4 \\ \text{or } 4z^4-4x^4y^4 &= (x^4-y^4)^2 \\ \text{or } z^4-x^4y^4 &= \left(\frac{x^4-y^4}{2}\right)^2. \end{aligned} \tag{12.5.2}$$

From Problem 12.5.2, we can assert that (12.5.2) has no non-zero solution. Thus at least one of $z,\ xy,\ x\pm y$ *is non-zero. Moreover, (12.5.1) and (12.5.2) have the same solutions. If* $x\neq y\neq 0$*, then* $x^4=y^4$*. Now from (12.5.1) we get,* $y^4=x^4=z^2$*. Thus the only possibility is* $x=y=z=1$*. Proceeding as above, in other cases too we can find* $x=y=z=1$.

Problem 12.5.7. *Show that the equation* $\dfrac{1}{x^4}+\dfrac{1}{y^4}=\dfrac{1}{z^2}$ *has no solution in positive integers.*

Solution 12.5.7. *Let the equation* $\frac{1}{x^4}+\frac{1}{y^4}=\frac{1}{z^2}$ *be solvable. Multiplying both sides by* $(xyz)^4$ *we obtain*

$$(yz)^4+(xz)^4=(x^2y^2z)^2. \tag{12.5.3}$$

It is of the form $a^4+b^4=c^2$*. In view of Theorem 12.4.1, we can say that the (12.5.3) has no non-zero solution for positive integers* yz, xz, x^2y^2z*. Consequently, our assumption proved to be wrong. This finishes our result.*

12.6 Exercises:

1. Find all Pythagorean triples (x, y, z) with $z \leq 40$.
2. Obtain all primitive Pythagorean triples x, y, z in which $x = 60$.
3. Show that if (x, y, z) is a primitive Pythagorean triple then, exactly one of x, y and z is divisible by 5.
4. Prove that in a primitive Pythagorean triple x, y, z the product xy is divisible by 12, hence $60 \mid xyz$.
5. Find all solutions in positive integers of the diophantine equation $x^2+3y^2=z^2$.
6. Prove that if x, y, z is a primitive Pythagorean triple in which the difference $z-y=2$, then $x=2t,\ y=t^2-1,\ z=t^2+1$ for some $t>1$.
7. Show that there exist infinitely many Pythagorean triples x, y, z in which x and y are consecutive triangular numbers. Exhibit three of these.
8. Find formulas for the integers of all Pythagorean triples (x, y, z) with $z = y+1$.

13

Integers as Sums of Squares

> *"Arithmetic is numbers you squeeze from your head to your hand to your pencil to your paper till you get the answer."*
>
> – Carl Sandburg

13.1 Introduction

Sum of squares of integers is the sum of two squares, three squares, four squares or n squares. In arithmetic operations we have sum of n terms. But there are many techniques for the calculation of sum of squares. In statistics and basic algebra, we have various results using sum of squares. From beginning many famous mathematicians like Euler, Lagrange and Gauss have contributed a lot to develop the concept of sum of squares. The basic problem they have encountered with is that, whether any integer can be expressed as sum of squares or not.

Obviously, we have shown that some numbers cannot be represented as sums of two squares; some numbers cannot be represented as sums of three squares, and all numbers can be represented as sums of four squares. Along the way, we also prove that numbers satisfying certain conditions can be represented as sums of two squares.

13.2 Sum of Two Squares

Throughout history, Mathematicians have been interested to find nature of numbers in many ways; mainly by addition and multiplication. Then, is it possible that these two operations be used together in the form of sum of squares? For instance, 25 can be expressed as $3^2 + 4^2$ but if we consider 11 then it cannot be written as the sum of two squares. Our future discussions will be based on the nature and properties of those integers which can be written as sum of two squares. To begin with, we will go for necessary and sufficient condition for which a positive integer can be expressed as sum of two squares. Our first theorem is the leading step towards this journey.

Theorem 13.2.1. *If p and q are two numbers such that each can be represented as the sum of two squares, then so is their product pq.*

Proof. Let $p = a^2 + b^2$ and $q = c^2 + d^2$ be the representation of p and q respectively, where a, b, c, d are integers. Now we have

$$\begin{aligned} pq &= (a^2 + b^2)(c^2 + d^2) \\ &= (ac + bd)^2 + (ac - bd)^2, \end{aligned}$$

where $ac + bd$ and $ac - bd$ are integers. Hence the proof. □

For further illustration if we choose $p = 5 = 2^2 + 1^2$ and $q = 10 = 3^2 + 1^2$ then we get, $pq = 50 = 49 + 1 = 7^2 + 1^2$. In this example we have seen that the prime number 5 has the sum of two squares representation. But this is not true for all primes. In fact $3 = c^2 + d^2$ has no integral solution. This leads us to our next theorem.

Theorem 13.2.2. *Any prime p satisfying $p \equiv 3 (\bmod\ 4)$ can not be represented as a sum of two squares.*

Proof. Suppose to the contrary, p can be written as $p = a^2 + b^2$ for some integers a and b. Now for $a \equiv 0, 1, 2$ or $3 (\bmod\ 4)$ we have $a^2 \equiv 0$ or $1 (\bmod\ 4)$. The same congruence relation holds for b. Adding both we get, $a^2 + b^2 \equiv 0, 1$ or $2 (\bmod\ 4)$. This contradicts the fact that $p \equiv 3 (\bmod\ 4)$. Thus p can not be represented as sum of two squares and we are done. □

The proof of the above theorem employs the fact that any prime which is congruent to 1 modulo 4 can be expressed as sum of two squares. We are now going to prove this statement. But to prove this we need to prove a wonderful lemma of congruence due to Norwegian Mathematician Alex Thue. In this lemma we have applied an important principle of mathematics namely Pigeon-hole principle.

Lemma 13.2.1. *(Thue) Let p be any prime and a be an integer with $\gcd(a, p) = 1$. Then there exists integers x and y with $0 < |x| < \sqrt{p}$ and $0 < |y| < \sqrt{p}$ so that $x \equiv ay (\bmod\ p)$.*

Proof. Let $k = [\sqrt{p}]$ be an integer such that $k^2 \leq p < (k+1)^2$. The number of pairs for which $0 \leq x \leq k$ and $0 \leq y \leq k$ is $(k+1)^2$. Here $(k+1)^2$ is greater than p so by Pigeon-hole principle there exists two pairs for which $x_1 - ay_1 \equiv x_2 - ay_2 (\bmod p)$. This implies $x_1 - x_2 \equiv ay_1 - ay_2 (\bmod p)$. Let $x = x_1 - x_2$ and $y = y_1 - y_2$, then we get $x \equiv ay (\bmod p)$. Here we need to show that $0 < |x| < k$ and $0 < |y| < k$ for $x, y \neq 0$. Let us consider one of them is zero then the other is also zero. If both x and y are zero then the pairs (x_1, y_1) and (x_2, y_2) are same. But this is not the case. Thus none of x or y is zero. This proves the lemma. □

Now we are in a position to prove the following theorem.

Theorem 13.2.3. *(Fermat) An odd prime p is expressible as a sum of two squares if and only if $p \equiv 1 (\bmod 4)$.*

Proof. Let us suppose that p can be written as sum of two squares, $p = a^2 + b^2$. As p is prime so $p \nmid a$ and $p \nmid b$. Now from theory of linear congruence there exists an integer c such that $bc \equiv 1 (\bmod p)$. Now multiplying both sides of $p = a^2 + b^2$ by c^2 and taking modulo p we have,

$$(ac)^2 \equiv -1 (\bmod p).$$

Here -1 is the quadratic residue of p. So by Legendre symbol we have, $(\frac{-1}{p}) = 1$ and applying Theorem 9.2.4 we get, $p \equiv 1 (\bmod 4)$.

For the converse part, let us assume that $p \equiv 1 (\bmod 4)$. An appeal to Theorem 9.2.4 gives $x^2 \equiv -1 (\bmod p)$ for an integer x. In view of Lemma 13.2.1 we can assert that for such an integer x there are integers a and b such that $0 < |a| < \sqrt{p}$, $0 < |b| < \sqrt{p}$ so that,

$$\begin{aligned} & a \equiv xb (\bmod p) \\ \Rightarrow\ & a^2 \equiv x^2 b^2 (\bmod p) \\ \Rightarrow\ & a^2 \equiv -b^2 (\bmod p) \\ \Rightarrow\ & a^2 + b^2 \equiv 0 (\bmod p). \end{aligned}$$

This shows that $p \big| (a^2 + b^2) \Rightarrow p \leq a^2 + b^2$. But $a^2 + b^2 < p + p = 2p$. Together we have $a^2 + b^2 = p$. □

From the last theorem it is clear that any prime p which is of the form $4k+1$, k being any integer, can be expressed as sum of two squares. For instance, if $p = 13$ then it can be written as $13 = 2^2 + 3^2$. Is the representation for $p = 13$ unique? We answer this below.

Corollary 13.2.1. *Any prime p of the form $4k+1$ can be expressed uniquely as sum of two squares of integers.*

Proof. Let us first consider $p = a^2 + b^2 = c^2 + d^2$ for some positive integers a, b, c, d. Then

$$\begin{aligned} a^2d^2 - b^2c^2 &= (p-b^2)d^2 - (p-d^2)b^2 \\ &= p(d^2 - b^2) \\ &\equiv 0(\mod p). \end{aligned}$$

This shows that either $ad \equiv bc(\text{mod } p)$ or $ad \equiv -bc(\text{mod } p)$. Since a, b, c, d are all less than $\sqrt{p}$ then this implies, either $ad - bc = 0$ or $ad + bc = p$.

If $ad + bc = p$ holds then we have

$$\begin{aligned} p^2 &= (a^2+b^2)(c^2+d^2) \\ &= (ad+bc)^2 + (ac-bd)^2 \\ &= p^2 + (ac-bd)^2. \end{aligned}$$

This gives $ac - bd = 0$ and it follows that either $ac = bd$ or $ad = bc$. Let $ad = bc$ holds then $a|bc$. Since $\gcd(a, b) = 1$ then it follows that $a|c$. Thus we have $c = ak$ for some integer k. So we can write $ad = b(ak) \Rightarrow d = bk$. But

$$p = c^2 + d^2 = k^2(a^2 + b^2),$$

implies $k = 1$. This leads to the fact that $a = c$, $b = d$. Again by similar arguments taking $ac = bd$ we get, $a = d$ and $b = c$. So the representation of p is unique. □

The subsequent part of this section addresses the characterization of those positive integers that can be expressed as sum of two squares. From Theorem 13.2.1 we can see that the square-free part of an integer is responsible for expressing as sum of two squares. In the following theorem we have shown the importance of square-free part of an integer.

Theorem 13.2.4. *Let n be a positive integer that can be expressed as $n = m^2k$ where k is square-free. Then n can be expressed as the sum of two squares if and only if k has no prime factor of the form $4t+3$, where t is non negative integer.*

Proof. If k has no prime factor of the form $4t+3$, then applying Theorem 13.2.3 we can say that each prime factor of k is of the form $4t+1$ and they can be expressed as sum of squares. Also by Theorem 13.2.1, their product is also sum of two squares. Thus k is of the form, $k = r^2 + s^2$ where r and s are integers. Therefore

$$n = m^2k = (mr)^2 + (ms)^2.$$

Conversely, let n be represented as sum of two squares $n = m^2k = a^2 + b^2$. Also let p be a prime factor of k. We are to show p is not of the form $4t + 3$. Let $d = \gcd(a, b)$ then $a = dk_1$, $b = dk_2$ where $\gcd(k_1, k_2) = 1$. Thus we have

$$d^2(k_1^2 + k_2^2) = m^2k.$$

As k is square-free so $d^2|m^2$, then we can write, $k_1^2 + k_2^2 = (\frac{m}{d})^2k = tk$ for some integer t. This shows that

$$k_1^2 + k_2^2 \equiv 0(\mod p).$$

As $\gcd(k_1, k_2) = 1$, then one of k_1 and k_2 is prime to p. Let k_1 be prime to p, then there exists k_1' such that $k_1k_1' \equiv 1(\text{mod } p)$. Therefore

$$\begin{aligned}(k_1k_1')^2 + (k_2k_1')^2 &\equiv 0(\mod p)\\ \Rightarrow (k_2k_1')^2 &\equiv -1(\mod p).\end{aligned}$$

This shows -1 is quadratic residue of p and $(-\frac{1}{p}) = 1$. Now applying Theorem 9.2.4 we get $p \equiv 1(\text{mod } 4)$. As p is arbitrary, this proves that k has no prime factor of the form $4t + 3$ for any integer $t(\geq 0)$. □

Example 13.2.1. *We are now going to illustrate the above theorem lucidly by some examples. Let us choose* $n = 245 = 7^2 \cdot 5 = 7^2(2^2 + 1^2) = 14^2 + 7^2$, *which can be expressed as sum of two squares. Here the prime factor* 7 *of the form* $4t + 3$ *is of even power. But if we consider this prime factor* 7 *as of odd power then it can not be expressed as sum of two squares.*

For example let $n = 1715 = 7^3 \cdot 5$ *and this can not be written as sum of two squares.*

From this above discussion yields the following corollary.

Corollary 13.2.2. *Any positive integer* n *can be represented as sum of two squares if and only if each of its prime factors of the form* $4t + 3$ *are of even powers.*

Finally we conclude the present section with the following theorem on representing an integer as difference of two squares.

Theorem 13.2.5. *Any positive integer* n *can be represented as difference of two squares if and only if* n *is not of the form* $4t + 2$ *for some integer* t.

Proof. Suppose n be represented as difference of two squares. Then $n = a^2 - b^2$ for some integers a and b. Here for any integer a we have, $a^2 \equiv 0$ or $1(\bmod 4)$. This follows that,

$$n = a^2 - b^2 \equiv 0, 1 \text{ or } 3(\bmod 4).$$

So n can not be of the form $4t + 2$ for any integer t.

Conversely, let n be not of the form $4t+2,\ t \in \mathbb{Z}$. Then $n \equiv 0, 1$ or $3(\bmod 4)$.

If $n \equiv 1$ or $3(\bmod 4)$, then $n+1$ and $n-1$ are both even integers. Thus n can be expressed as

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2.$$

Also if $n \equiv 0(\bmod 4)$ then we have

$$n = \left(\frac{n}{4}+1\right)^2 - \left(\frac{n}{4}-1\right)^2.$$

This shows that n can be expressed as difference of two squares. □

To illustrate this theorem, let us take $n = 15$ and it can be expressed as $15 = 8^2 - 7^2$. But $n = 14$ can not be expressed as the difference of two squares. Taking advantage of the treatment of Theorem 13.2.5 yields an obvious corollary.

Corollary 13.2.3. *An odd prime is the difference of squares of two successive numbers.*

13.3 Worked out Exercises

Problem 13.3.1. *Represent each of the primes* $113, 229$ *and* 373 *as a sum of two squares.*

Solution 13.3.1. *Note that* $113 \equiv 1(\bmod 4)$, $229 \equiv 1(\bmod 4)$ *and* $373 \equiv 1(\bmod 4)$. *Thus the given odd primes are expressible in the form* $4t+1$. *Applying Theorem 13.2.3 we see that these numbers can be expressed as sum of two squares. The expressions are,* $113 = 8^2 + 7^2$, $229 = 15^2 + 2^2$ *and* $373 = 18^2 + 7^2$.

Problem 13.3.2. *Show that a prime* p *can be written as sum of two squares if and only if the congruence* $x^2 + 1 \equiv 0(\bmod p)$ *admits a solution.*

Solution 13.3.2. *Let* $p = a^2 + b^2$ *be the prime number where* a, b *are positive integers. Then* $a^2 + b^2 \equiv 0(\bmod p)$ *with* $b \not\equiv 0(\bmod p)$. *On dividing both sides of the congruence by* b^2 *yields,*

$$\left(\frac{a}{b}\right)^2 + 1 \equiv 0(\bmod p).$$

This shows that $x = \frac{a}{b}$ *is the solution of* $x^2 + 1 \equiv 0 \pmod p$.

Conversely, let $x^2 + 1 \equiv 0 \pmod p$ *admits a solution. This implies that* -1 *is a quadratic residue modulo* p. *By Legendre symbol we have* $(\frac{-1}{p}) = 1$. *In view of Theorem 9.2.4, we get* $p \equiv 1 \pmod 4$. *This proves that* p *can be expressed as sum of two squares.*

Problem 13.3.3. *Prove that the positive integer* n *as many representations as the sum of two squares as does the integer* $2n$.

Solution 13.3.3. *Let* n *be a positive integer which can be represented as* $n = a^2 + b^2$ *for any integer* a *and* b. *For this representation of* n *we get,*

$$2n = (a+b)^2 + (a-b)^2$$

where both $a+b$ *and* $a-b$ *are integers. From these two representations of* n *and* $2n$, *we can say that* n *has as many as representations as the sum of two squares as does* $2n$ *and vice versa.*

Problem 13.3.4. *Show that of any four consecutive integers, at least one of them is not represented as a sum of two squares.*

Solution 13.3.4. *Let* n *be an integer which can be written as sum of two squares. Then* n *is of the form* $n = a^2 + b^2$ *for any integers* a *and* b. *Here both* a^2 *and* b^2 *are congruent to* 0 *or* 1 *modulo* 4. *This shows that* $a^2 + b^2$ *is congruent to* $0, 1$ *or* 2 *modulo* 4.

If $n \equiv 0 \pmod 4$, *then* $n + 3 \equiv 3 \pmod 4$.
If $n \equiv 1 \pmod 4$, *then* $n + 2 \equiv 3 \pmod 4$.
If $n \equiv 2 \pmod 4$, *then* $n + 1 \equiv 3 \pmod 4$.

Thus for all these cases there is at least one integer among $n, n+1, n+2, n+3$ *which is congruent to* 3 *modulo* 4 *and that integer can not be written as sum of two squares.*

Problem 13.3.5. *If a positive integer* n *is not the sum of squares of two integers then prove that* n *can not be represented as sum of two squares of rational numbers.*

Solution 13.3.5. *As* n *can not be written as sum of two squares, it has a prime factor* p *of the form* $4t+3$ *for any integer* $t(\geq 0)$. *Further, referring to Corollary 13.2.2, we can say that* p *occurs in odd powers. This shows* $p^k | n$ *for some odd integer* k. *If* n *can be expressed as* $n = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2$ *for some integers* a, b, c, d *with* $b, d \neq 0$, *we get* $n(bd)^2 = (ad)^2 + (cd)^2$. *Here in the left hand side,* p *occurs to be an odd power but in the right hand side it happens to be an even power [by Corollary 13.2.2]. This is not possible. Thus* n *can not be written as sum of two squares of rational numbers.*

Problem 13.3.6. *A positive integer is representable as the difference of two squares if and only if it is the product of two factors that are both even or both odd.*

Solution 13.3.6. *Let n be the positive integer, which can be represented as difference of two squares. Thus we have,*

$$n = a^2 - b^2 = (a+b)(a-b).$$

Let $a+b = 2m+1$ and $a-b = 2m'$. This implies $a = \dfrac{2(m+m')+1}{2}$ and $b = \dfrac{2(m-m')+1}{2}$. Therefore

$$\begin{aligned} n &= a^2 - b^2 \\ &= \frac{1}{4}[4(m+m')^2 + 4(m+m') + 1 - 4(m-m')^2 - 4(m-m') - 1] \\ &= 8m'(2m+1). \end{aligned}$$

Comparing we get $a - b = 8m'$, which is not true. This asserts that both $a+b$ and $a-b$ are either even or odd.

Conversely, let $n = m_1 m_2$ where both m_1 and m_2 are even say $m_1 = 2k_1$ and $m_2 = 2k_2$. Then we get

$$\begin{aligned} n &= \frac{1}{4}[(m_1+m_2)^2 - (m_1-m_2)^2] \\ &= [(k_1+k_2)^2 - (k_1-k_2)^2]. \end{aligned}$$

If both m_1 and m_2 are odd, say $m_1 = 2k_1+1$ and $m_2 = 2k_2+1$, then we get

$$\begin{aligned} n &= \frac{1}{4}[(m_1+m_2)^2 - (m_1-m_2)^2] \\ &= [\{2(k_1+k_2)+2\}^2 - 4(k_1-k_2)^2] \\ &= [(k_1+k_2+1)^2 - (k_1-k_2)^2]. \end{aligned}$$

This shows that in both the cases the integer n can be expressed as difference of two squares.

Problem 13.3.7. *Verify that 45 is the smallest positive integer admitting three distinct representations as the difference of two squares.*

Solution 13.3.7. *Considering the Problem(13.3.6), we can say that both the factors $a+b$ and $a-b$ are either even or odd, for any integer $n = a^2 - b^2$. Here $n = 45$ can be written as 1×45 or 3×15 or 5×9. Thus the distinct representations of 45, as the difference of two squares are $n = 23^2 - 22^2$ or $9^2 - 6^2$ or $7^2 - 2^2$.*

Problem 13.3.8. *Express the integers* 650 *and* 1450 *as sum of two squares.*

Solution 13.3.8. *Note that* $13 = 3^2 + 2^2,\ 29 = 5^2 + 2^2$ *and* $50 = 7^2 + 1^2$. *Now*

$$\begin{aligned}650 &= 13 \cdot 50\\ &= (3^2+2^2)(7^2+1^2)\\ &= (3\cdot 1 + 2\cdot 7)^2 + (3\cdot 7 - 2\cdot 1)^2 \ [\textit{Why!}]\\ &= 17^2 + 19^2.\\ 1450 &= 29 \cdot 50\\ &= (5^2+2^2)(7^2+1^2)\\ &= (5\cdot 1 + 2\cdot 7)^2 + (5\cdot 7 - 2\cdot 1)^2 \ [\textit{Why!}]\\ &= 19^2 + 33^2.\end{aligned}$$

13.4 Sum of More than Two Squares

The foregoing section describes the aspects of those integers which can be written as sum of two squares. But there exist few integers which can not be expressed as sum of two squares. For instance, if we consider 26 then $26 = 1^2 + 3^2 + 4^2$. The present section deals with those types of integers which can be expressed as sum of three squares or more than that.

We started with the study of the existence of integers which can be expressed as sum of three squares of integers. We pave the way with a significant lemma.

Lemma 13.4.1. *An integer congruent to* 7 *modulo* 8 *cannot be represented as sum of three squares of integers.*

Proof. Suppose that an integer N of the form $N \equiv 7(\mod 8)$ can be expressed as $N = x^2 + y^2 + z^2$ where $x, y, z \in \mathbb{Z}$. We note that square of any integer is congruent to $0, 1$ or 4 modulo 8. Applying these two assertions we can say that N is congruent to $0, 1, 2, 3, 4, 5$ or 6 modulo 8. This contradicts our assumption and hence we are done. □

Taking the lemma into consideration, we can prove the following theorem.

Theorem 13.4.1. *The positive integers of the form* $4^a(8b+7)$, *where* a *and* b *are non negative integers, cannot be expressed as sum of three squares of integers.*

Proof. Here the positive integer N is of the form $4^a(8b+7)$, where a and b are non negative integers. Let us consider $a \geq 1$ and $N = x^2 + y^2 + z^2$. Then $N \equiv 0($

mod 4) implies x, y and z must be even. Putting $x = 2x_1, y = 2y_1$ and $z = 2z_1$ we get,

$$4^{a-1}(8b+7) = x_1^2 + y_1^2 + z_1^2$$

for some integers x_1, y_1 and z_1.

Again, consider $a - 1 \geq 1$. Then proceeding as above and reducing the exponent of 4 we obtain $a = 0$. This concludes that $N \equiv 7 (\mathrm{mod}\ 8)$. Thus N can be expressed as sum of three squares of integers. But this contradicts the Lemma 13.4.1. This completes the proof. □

The foregoing theorem highlights the fact that there are integers which can not be written as sum of three squares. For instance, if we choose $N = 28$ then we see that it can not be written as sum of three squares. But 28 can be written as $28 = 5^2 + 1^2 + 1^2 + 1^2$. Here 28 has been written as sum of four squares. A natural question is to ask whether every integer can be written as sum of four squares or not. We settle this below.

Theorem 13.4.2. *If p and q be two positive integers which can be expressed as sum of four squares, then their product is also so.*

Proof. Let $p = p_1^2 + p_2^2 + p_3^2 + p_4^2$ and $q = q_1^2 + q_2^2 + q_3^2 + q_4^2$. Now we can have

$$\begin{aligned} pq &= (p_1^2 + p_2^2 + p_3^2 + p_4^2)(q_1^2 + q_2^2 + q_3^2 + q_4^2) \\ &= (p_1q_1 + p_2q_2 + p_3q_3 + p_4q_4)^2 + (p_1q_2 - q_1p_2 + p_3q_4 - p_4q_3)^2 \\ &\quad + (p_1q_3 - q_1p_3 + p_4q_2 - p_2q_4)^2 + (p_1q_4 - p_4q_1 + p_2q_3 - p_3q_2)^2. \end{aligned}$$

Here the above identity can be verified by simple calculation. This shows pq can also be written as sum of four squares. □

Consider $p = 12$ and $q = 13$. Then $12 = 3^2 + 1^2 + 1^2 + 1^2$ and $13 = 3^2 + 2^2 + 0^2 + 0^2$. Here

$$\begin{aligned} 12 \cdot 13 &= (3^2 + 1^2 + 1^2 + 1^2)(3^2 + 2^2 + 0^2 + 0^2) \\ &= (9+2)^2 + (6-3)^2 + (2-3)^2 + (-3-2)^2 \\ &= 121 + 9 + 1 + 25 = 156. \end{aligned}$$

This establishes the fact behind the above theorem.

We are now going to conclude this section by proving the fact that any integer can be expressed as sum of four squares of integers. To prove this assertion, we need some lemmas.The fundamental theorem of arithmetic says that every integer greater than 1 can be expressed as a product of powers of distinct primes. Combining this with the assertion of Theorem 13.4.2, if we can show that any prime can be written as sum of four squares, then we are done. Here for the prime $p = 2$, we have $2 = 1^2 + 1^2 + 0^2 + 0^2$. So the last assertion is trivially true. To fulfill the purpose for odd primes, let us state and prove the following lemmas.

Lemma 13.4.2. *If p is an odd prime, then there exists an integer $m < p$ such that*

$$1 + x^2 + y^2 = mp,\ 0 < m < p,$$

for some integers x and y with $0 \leq x \leq \frac{p}{2}$ and $0 \leq y \leq \frac{p}{2}$ respectively.

Proof. Let us consider x from the set $\{0, 1, 2, \cdots, \frac{p-1}{2}\}$. Then x^2 have all of different congruences modulo p. If not, let us consider $x_1^2 \equiv x_2^2 (\bmod p)$, then $p|(x_1 - x_2)(x_1 + x_2) \Rightarrow x_1 \equiv \pm x_2 (\bmod p)$. This is not possible.

Applying the same idea for $y = 0, 1, 2, \cdots \dfrac{p-1}{2}$, the numbers $-1 - y^2$ are all incongruent modulo p. Thus we have two sets of $\dfrac{p+1}{2}$ numbers of incongruent modulo p for x and y respectively. But in totality there are $p + 1$ number of elements in these two sets where only p number of elements are residue modulo p. This shows that there exists at least one element from $\big\{0, 1, 2, \cdots \dfrac{p-1}{2}\big\}$ for which x^2 is congruent to $-1 - y^2$ modulo p. Hence

$$x^2 \equiv -1 - y^2 (\bmod p) \Rightarrow 1 + x^2 + y^2 \equiv mp.$$

Now $x^2 < \big(\dfrac{p}{2}\big)^2$ and $y^2 < \big(\dfrac{p}{2}\big)^2$ together implies

$$mp = 1 + x^2 + y^2 < 1 + 2\Big(\frac{p}{2}\Big)^2 < p^2.$$

Thus $m < p$. ☐

For instance, if we choose $p = 7$ then we have $1 + 2^2 + 4^2 = 3 \times 7$. Now using this lemma we are going to prove the next one.

Lemma 13.4.3. *For any odd prime p, there exists an integer $m < p$ such that mp can be expressed as sum of four squares.*

Proof. From the last lemma, for any two integers s and t with $0 \leq s < \dfrac{p}{2}$ and $0 \leq t < \dfrac{p}{2}$ such that

$$s^2 + t^2 + 1^2 + 0^2 = mp \text{ where } m < p.$$

This finishes the proof. ☐

Finally, by virtue of last two lemmas we are going to show the expression for any odd prime as sum of four squares.

Lemma 13.4.4. *Any odd prime p can be expressed as sum of four squares of integers.*

Proof. With the aid of Lemma 13.4.3, for any odd prime p we can say that there exists an integer m with $m < p$ such that

$$x^2 + y^2 + z^2 + w^2 = mp$$

where x, y, z, w are integers. To prove this lemma, it's suffices to show that $m = 1$. For that assume $m > 1$.

If m is even then three possible cases may arise: all the integers x, y, z, w are even; all are odd; any two of them are even and other two are odd. For all those possibilities we can arrange them as $x \equiv y (\bmod 2)$ and $z \equiv w (\bmod 2)$. It follows that $\frac{x-y}{2}, \frac{x+y}{2}, \frac{z-w}{2}, \frac{z+w}{2}$ are all integers and

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 = \left(\frac{m}{2}\right)p.$$

This contradicts the minimality of m.

If m is odd then there exists integers $\alpha, \beta, \gamma, \delta$ such that $x \equiv \alpha (\bmod m)$, $y \equiv \beta (\bmod m)$, $z \equiv \gamma (\bmod m)$ and $w \equiv \delta (\bmod m)$ with $-(\frac{m}{2}) < \alpha, \beta, \gamma, \delta < \frac{m}{2}$. Now we have

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv x^2 + y^2 + z^2 + w^2 (\bmod m)$$

and this implies, $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = tm$ for some integer t and $0 \leq \alpha^2 + \beta^2 + \gamma^2 + \delta^2 < 4\left(\frac{m}{2}\right)^2 = m^2 \Rightarrow 0 \leq t < m$.

Here $t > 0$, since for $t = 0$ we have $\alpha = \beta = \gamma = \delta = 0$ and consequently $x \equiv y \equiv z \equiv w \equiv 0 (\bmod m)$. This shows that $m^2 \mid mp$ which is not possible as $1 < m < p$. Again by Theorem 13.4.2 we have

$$m^2 tp = (tm)(mp) = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)(x^2 + y^2 + z^2 + w^2).$$

This shows $tp = A^2 + B^2 + C^2 + D^2$ where

$$\begin{aligned} A &= \frac{(x\alpha + y\beta + z\gamma + w\delta)}{m} \\ B &= \frac{(x\beta - y\alpha + z\delta - w\gamma)}{m} \\ C &= \frac{(x\gamma - y\delta - z\alpha + w\beta)}{m} \\ D &= \frac{(x\delta + y\gamma - z\beta - w\alpha)}{m}. \end{aligned}$$

Again this contradicts the choice of m. Thus m must be 1. This proves the lemma. □

We are now in a position to state the fundamental theorem about representation of any integer as sum of four squares. The proof follows from the Theorem 13.4.2, Lemma 13.4.3 and Lemma 13.4.4 together with fundamental theorem of arithmetic.

Theorem 13.4.3. *Every positive integer is the sum of squares of four integers.*

13.5 Worked out Exercises

Problem 13.5.1. *If* $p = q_1^2 + q_2^2 + q_3^2$ *where* p, q_1^2, q_2^2, q_3^2 *are all primes, show that some* $q_i = 3$ *for* $i = 1, 2, 3$.

Solution 13.5.1. *Observe that* p, q_1, q_2, q_3 *are primes. Then each* q_i *is either congruent to* 0 *or* 1 *modulo* 3. *If all* q_i *congruent* 1 *modulo* 3, *then* $p \equiv 1 + 1 + 1 (\text{mod } 3)$. *Thus* $p \equiv 0 (\text{mod } 3)$ *and since* p *is prime,* $p = 3$ *is the only possibility. Note that* $3 = 1^2 + 1^2 + 1^2$ *implies* $q_i = 1$ *for* $i = 1, 2, 3$. *This is not possible as* q_i*'s are primes. So atleast one of* q_i*'s is congruent to* 0 *modulo* 3. *Since* q_i*'s are prime numbers, hence the result follows.*

Problem 13.5.2. *For a given positive integer show that* n *or* $2n$ *is a sum of three squares.*

Solution 13.5.2. *If* n *is sum of three squares, then there is nothing to prove. Let* n *cannot be expressed as sum of three squares. Then it is of the form* $4^a(8b + 7)$ *for some non negative integers* a *and* b. *Now* $2n = 2 \cdot 4^a(8b+7)$ *and if* $2n$ *cannot be written as sum of three squares, then it is of the form* $4^e(8d+7)$ *for some non negative integers* c *and* d. *Comparing we get* $2 \cdot 4^a = 4^e$, *which is impossible. Thus* $2n$ *is not of the form* $4^e(8d + 7)$ *and hence it can be expressed as sum of three squares.*

Problem 13.5.3. *Represent the integers* 90 *and* 23 *as the sum of three squares.*

Solution 13.5.3. *Since* $90 \equiv 2 (\text{mod } 8)$, *therefore from Lemma 13.4.1 it follows that* 90 *can be expressed as sum of three squares. In fact we have* $90 = 8^2+5^2+1^2$.

Again, $23 \equiv 7 (\text{mod } 8)$. *In view of Lemma 13.4.1, we can say that* 23 *cannot be expressed as sum of three squares of integers.*

Problem 13.5.4. *Verify that every positive odd integer is of the form* $a^2 + b^2 + 2c^2$, *where* a, b, c *are integers.*

Solution 13.5.4. *For any positive integer n, let $2n+1$ be the required positive integer. Now $4n+2$ is not of the form $4^a(8b+7)$ for some positive integers a and b. So by virtue of Theorem 13.4.1, we can say that $4n+2$ can be expressed as sum of three squares.*

Let $4n+2 = x^2+y^2+z^2$, for some integers x, y and z. Here exactly two amongst x^2, y^2, z^2 are congruent to 1 modulo 4. Let us consider x, y be two odd integers and z be even. Now

$$2n+1 = \Big(\frac{x+y}{2}\Big)^2 + \Big(\frac{x-y}{2}\Big)^2 + 2\Big(\frac{z}{2}\Big)^2.$$

Thus $2n+1 = a^2+b^2+2c^2$, where $a = \frac{x+y}{2}$, $b = \frac{x-y}{2}$ and $c = \frac{z}{2}$ are integers.

Problem 13.5.5. *Prove or disprove that the sum of two integers each representable as the sum of three squares of integers is also representable as sum of three squares.*

Solution 13.5.5. *In general, the statement is not true. Choose $4 = 2^2+0^2+0^2$ and $3 = 1^2+1^2+1^2$. Then their sum $3+4=7$ can be written as $7 \equiv 7 \pmod 8$. From Lemma 13.4.1, we can say that 7 cannot be expressed as sum of three squares.*

Problem 13.5.6. *Express 21 and 89 as the sum of four squares.*

Solution 13.5.6. *Here $21 = 3\times 7$ and both 3 and 7 are odd primes. By virtue of Lemma 13.4.4, both 3 and 7 can be expressed as sum of four squares. Moreover, from Theorem 13.4.2 we have $21 = 3\times 7$ and it can be expressed as sum of four squares. The expression is $21 = 4^2+2^2+1^2+0^2$.*

Furthermore, 89 is an odd prime. Then from Lemma 13.4.4, we can assert that 89 can also expressed as sum of four squares and it is of the form, $89 = 9^2+2^2+2^2+0^2$.

Problem 13.5.7. *Write $105 = 7\times 15$ and $510 = 15\times 34$ as the sum of four squares.*

Solution 13.5.7. *Here $15 = 3^2+2^2+1^2+1^2$, $7 = 2^2+1^2+1^2+1^2$ and $34 = 4^2+4^2+1^2+1^2$. Taking help of proof of the Theorem 13.4.2 we get,*

$$\begin{aligned}
105 &= 15\times 7\\
&= (3^2+2^2+1^2+1^2)(2^2+1^2+1^2+1^2)\\
&= (2\cdot 3+2\cdot 1+1\cdot 1+1\cdot 1)^2+(3\cdot 1-2\cdot 2+1\cdot 1-1\cdot 1)^2\\
&\quad +(3\cdot 1-2\cdot 1+1\cdot 1-2\cdot 1)^2+(3\cdot 1-2\cdot 1+2\cdot 1-1\cdot 1)^2\\
&= 10^2+2^2+1^2+0^2.
\end{aligned}$$

Similarly, we can find the expression for $510 = 15\times 34$.

Problem 13.5.8. *Show that every integer* n, $n \geq 170$, *is the sum of the squares of five positive integers.*

Solution 13.5.8. *Note that any integer can be expressed as sum of four squares. Then choose* $m = n - 169$, *which can be expressed as sum of four squares. Let* $m = x^2 + y^2 + z^2 + w^2$ *for some integers* x, y, z *and* w.

If x, y, z *are* 0, *then* $n = w^2 + 169 = w^2 + 10^2 + 8^2 + 2^2 + 1^2$.

If x, y *are* 0, *then* $n = z^2 + w^2 + 169 = z^2 + w^2 + 12^2 + 4^2 + 3^2$.

If x *is* 0, *then* $n = y^2 + z^2 + w^2 + 169 = y^2 + z^2 + w^2 + 12^2 + 5^2$.

If none are 0, *then* $n = x^2 + y^2 + z^2 + w^2 + 169 = x^2 + y^2 + z^2 + w^2 + 13^2$.

Problem 13.5.9. *A prime* p *can be represented as the difference of two cubes if and only if it is of the form* $p = 3k(k+1) + 1$, *for some* k. *Hence express* 7 *as the difference of two cubes.*

Solution 13.5.9. *Let* p *be a prime which can be expressed as difference of two cubes. Then we have* $p = a^3 - b^3 = (a - b)(a^2 + ab + b^2)$. *Since* p *is prime, therefore either* $a - b = 1$ *or* $a^2 + ab + b^2 = 1$.

If $a^2 + ab + b^2 = 1$, *then* $a = 1$ *and* $b = -1$ *gives* $p = 2 = 1^3 - (-1)^3$ *which is not of the form* $3k(k + 1) + 1$.

If $a - b = 1$, *then* $a = 1 + b$ *which gives* $p = (1 + b)^3 - b^3 = 3b(b + 1) + 1$ *for any integer* b.

Thus p *is of the form* $3k(k + 1) + 1$ *for any integer* k.

Conversely, if $p = 3k(k + 1) + 1$, *then* $p = (k + 1)^3 - k^3$ *for any integer* k. *Thus* p *can be expressed as difference of two cubes.*

For the second part, pick $k = 1$. *Then* $p = 3 \cdot 1(1+1)+1 = 7$ *can be expressed as* $7 = 2^3 - 1^3$.

13.6 Exercises:

1. Show that each of the integers 2^n, where $n = 1, 2, 3, \cdots$, can be expressed as sum of two squares.

2. Prove that every Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 1$, can be expressed as the sum of two squares.

3. Express 101 and 490 as the sum of two squares.

4. If n is a triangular number, show that each of the three successive integers $8n^2, 8n^2 + 1, 8n^2 + 2$ can be written as a sum of two squares.

5. Prove that a positive even integer can be written as the difference of two squares if and only if it is divisible by 4.

6. Express 11 and 28 as the sum of three squares if possible.

7. Show that every positive integer is either of the form $a^2 + b^2 + c^2$ or $a^2 + b^2 + 2c^2$, where a, b, c are integers.

8. Show that the only prime p that is representable as the sum of two positive cubes is $p = 2$.

9. Express 12 and 99 as the sum of four squares.

10. Prove that no positive integer n, $n = \pm 4 (\text{mod } 9)$, is the sum of three cubes.

14

Certain Applications on Number Theory

"Mathematics is the language of nature."

– Leonardo Fibonacci

14.1 Fibonacci Numbers

The word Fibonacci is coined after the mathematician Leonardo Fibonacci, who in the 12th century, get obstructed while studying a curious problem. Fibonacci started with a pair of fictional and slightly unbelievable baby rabbits, a baby boy rabbit and a baby girl rabbit. After one month, they were fully grown and in the next month two more baby rabbits (again a boy and a girl) were born. The succeeding month these babies were fully grown and the first pair had two more baby rabbits (again, a boy and a girl). By similar manner, the next month the two adult pairs each have a pair of baby rabbits and the babies from last the month mature. Fibonacci asked how many rabbits a single pair can produce after a year (every month each adult pair produces a mixed pair of baby rabbits who mature the next month). He realised that the number of adult pairs in a given month is the total number of rabbits (both adults and babies) in the previous month. Writing A_n for the number of adult pairs in the nth month and R_n for the total number of pairs in the nth month, this gives $A_n = R_{n-1}$.

Fibonacci also realised that the number of baby pairs in a given month is the number of adult pairs in the previous month. Writing Fibonacci also realised that the number of baby pairs in a given month is the number of adult pairs in the previous month. Writing B_n for the number of baby pairs in the nth month, this gives for the number of baby pairs in the nth month, this gives $B_n = A_{n-1} R_{n-2}$.

Therefore the total number of pairs of rabbits (adult+baby) in a particular month is the sum of the total pairs of rabbits in the previous two months: $R_n = A_n + B_n = R_{n-1} + R_{n-2}$.

Starting with one pair, the sequence we generate is exactly the sequence at the start of this article. And from that we can see that after twelve months there will be 144 pairs of rabbits.

Theorem 14.1.1. *In a Fibonacci sequence, the successive terms are relatively prime.*

Proof. Its suffices to show that for a Fibonacci sequence, $\gcd(V_n, V_{n+1}) = 1 \ \forall n \geq 1$. On the contrary, let $d = \gcd(V_n, V_{n+1})$, $d > 1$. Then $d \big| V_n$ and $d \big| V_{n+1}$. Also, $d \big| (V_{n+1} - V_n) \Rightarrow d \big| V_{n-1}$. Now, $V_n - V_{n-1} = V_{n-2}$. Combining $d \big| V_n$ and $d \big| V_{n-1}$ yield $d \big| V_{n-2}$. Similar argument generates

$$d \big| V_{n-3}, d \big| V_{n-4}, \ldots, d \big| V_3, d \big| V_2, d \big| V_1.$$

But, $V_1 = 1$ and $d \big| V_1$ leads to contradiction. Hence the proof. □

The identity

$$V_{m+n} = V_{m-1} V_n + V_m V_{n+1} \tag{14.1.1}$$

is primal to bring out many spectacular features of the Fibonacci sequence. For fixed $m \geq 2$, we proceed by mathematical induction on n. For $n = 1$, the identity takes the form

$$V_{m+1} = V_{m-1} V_1 + V_m V_2 = V_{m-1} + V_m,$$

which is trivially true. Assume that the identity is true for $n = k$. Then

$$V_{m+k} = V_{m-1} V_k + V_m V_{k+1} \ \& \tag{14.1.2}$$

$$V_{m+(k-1)} = V_{m-1} V_{k-1} + V_m V_k. \tag{14.1.3}$$

Combining (14.1.2) and (14.1.3) gives

$$V_{m+k} + V_{m+(k-1)} = V_{m-1}(V_k + V_{k-1}) + V_m(V_{k+1} + V_k).$$

Following the definition of Fibonacci sequence, the foregoing equation is the same as

$$V_{m+k+1} = V_{m-1} V_{k+1} + V_m V_{k+2},$$

which is the desired identity with $n = k + 1$. Hence by induction method the identity is true for $m \geq 2$ and $n \geq 1$.

Theorem 14.1.2. *For* $m \geq 1, n \geq 1,\ V_m \big| V_{mn}$.

Proof. Here we argue by principles of mathematical induction on n. For $n = 1$, the theorem is trivially true. Let $V_m \big| V_{mn}$ be true for $n = 1, 2, 3, \ldots, k$. An appeal to the identity (14.1.1) yields

$$V_{m(k+1)} = V_{mk+m} = V_{mk-1} V_m + V_{mn} V_{m+1}.$$

By induction hypothesis,

$$V_m \big| V_{mk} \Rightarrow V_m \big| V_{mk-1} V_m + V_{mn} V_{m+1} \Rightarrow V_m \big| V_{m(k+1)}.$$

Hence the proof. □

Lemma 14.1.1. *If* $m = qn + r$, *then* $\gcd(V_m, V_n) = \gcd(V_r, V_n)$.

Proof. Here, we have

$$\begin{aligned} \gcd(V_m, V_n) &= \gcd(V_{qn+r}, V_n), \\ &= \gcd(V_{qn-1} V_r + V_{qn} V_{r+1}, V_n) \text{ by identity(14.1.1).} \end{aligned}$$

Combining the fact that $\gcd(a + c, b) = \gcd(a, b)$ whenever $b \big| c$ and the foregoing theorem yields,

$$\gcd(V_{qn-1} V_r + V_{qn} V_{r+1}, V_n) = \gcd(V_{qn-1} V_r, V_n).$$

Claim: $\gcd(V_{qn-1}, V_n) = 1$. To fulfill this, consider $\gcd(V_{qn-1}, V_n) = d$. Combining $d \big| V_n$ and $V_n \big| V_{qn}$ imply $d \big| V_{qn}$ and therefore, d is a common divisor of the Fibonacci numbers V_{qn-1} and V_{qn}. Since successive Fibonacci numbers are relatively prime, this results in $d = 1$. Finally, with the help of the fact $\gcd(a, c) = 1 \Rightarrow \gcd(a, bc) = \gcd(a, b),\ \forall a, b, c \in \mathbb{Z}$, we obtain the desired lemma. □

Theorem 14.1.3. *The greatest common divisor of two Fibonacci numbers is again a Fibonacci number.*

Proof. Its suffices to show that $\gcd(V_m, V_n) = V_d$ where $\gcd(m, n) = d$ and V_m, V_n and V_d are Fibonacci numbers. If possible, set $m \geq n$. An appeal to Euclidean algorithm to m and n gives

$$\begin{aligned} m &= q_1 n + r_1, \quad 0 < r_1 < n \\ n &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

By the last lemma, we obtain

$$\begin{aligned} \gcd(V_m, V_n) &= \gcd(V_{r_1}, V_n) \\ &= \gcd(V_{r_1}, V_{r_2}) \\ &= \cdots = \gcd(V_{r_{n-1}}, V_{r_n}). \end{aligned}$$

Now addressing Theorem 14.1.2, we have

$$r_n \,\big|\, r_{n-1} \Rightarrow V_{r_n} \,\big|\, V_{r_{n-1}} \text{ (How!)}.$$

But $r_n = \gcd(m, n)$(Why!). Blending all the facts generate the desired one. □

Theorem 14.1.4. *Let* $n \in \mathbb{Z}^+$ *and* $\alpha = \frac{1+\sqrt{5}}{2}$. *Then* $V_n > \alpha^{n-2}$, $\forall\, n \geq 3$.

Proof. We proceed by mathematical induction on n to obtain the desired inequality. For $n = 3$, $V_3 = 2 > \alpha$. So the inequality prevails for $n = 3$. Assume the inequality holds for all integers k with $k \leq n$. Then $\alpha^{k-2} < V_k$. Since $\alpha = \frac{1+\sqrt{5}}{2}$ is one of the roots of $x^2 - x - 1 = 0$, therefore $\alpha^2 - \alpha - 1 = 0$. Hence $\alpha^2 = k + 1$. So

$$\alpha^{n-1} = \alpha^2 \cdot \alpha^{n-3} = (\alpha + 1) \cdot \alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}.$$

By induction, we have the following inequalities

$$\alpha^{n-2} < V_n, \ \alpha^{n-3} < V_{n-1}.$$

Thus,

$$\alpha^{n-1} < V_n + V_{n-1} = V_{n+1} \Rightarrow V_{n+1} > \alpha^{n-1}.$$

Hence the inequality is true for $n = k + 1$. So our task is complete. □

Theorem 14.1.5. *Let* V_{k+1} *and* V_{k+1} *be successive terms of the Fibonacci sequence. Then the Euclidean algorithm takes exactly* k *divisions to show that* $\gcd(V_{k+1}, V_{k+2}) = 1$.

Proof. Taking aid of Euclidean algorithm and the defining relation for Fibonacci sequence $V_n = V_{n-1} + V_{n-2}$ at every step, we find that

$$\begin{aligned} V_{n+2} &= V_{n+1} \cdot 1 + V_n \\ V_{n+1} &= V_n \cdot 1 + V_{n-1} \\ \vdots &= \vdots \\ V_4 &= V_3 \cdot 1 + V_2 \\ V_3 &= V_2 \cdot 2 + 0 \\ V_2 &= 0 \cdot 2 + V_1 = 2. \end{aligned}$$

Hence the Euclidean algorithm takes exactly n-divisions to show $\gcd(V_{k+1}, V_{k+2}) = 1$. □

Our next discussions will be based on $Lamé's$ theorem, first proved by a French Mathematician Gabriel Lamé of 19th century, which calculates the number the number of division required to find greatest common divisor by means of Euclidean Algorithm.

Theorem 14.1.6. *Lamé's Theorem: The number of divisions needed to find the greatest common divisor of two positive integers using the Euclidean Algorithm, does not exceed five times the number of digits in the smaller of the two digits.*

Proof. Taking into consideration, the Euclidean algorithm to find the greatest common divisor of $a = r_0$ and $b = r_1$ with $a > b$, we get the following set of equations;

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, & 0 &\leq r_2 \leq r_1. \\
r_1 &= r_2 q_2 + r_3, & 0 &\leq r_3 \leq r_2. \\
r_2 &= r_3 q_2 + r_4, & 0 &\leq r_4 \leq r_3. \\
\vdots &= \vdots \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1}, & 0 &\leq r_{n-1} \leq r_{n-2}. \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 &\leq r_n \leq r_{n-1}. \\
r_{n-1} &= r_n q_n.
\end{aligned}$$

We have used n-divisions. We note that each of the quotients $q_1, q_2, \ldots, q_{n-1}$ is greater than or equal to 1 and $q_n \geq 2$, since $r_n < r_{n-1}$. Hence

$$\begin{aligned}
& r_n \geq 1 = V_2, \\
& r_{n-1} \geq 2r_n \geq 2V_2 = V_3, \\
& r_{n-2} \geq r_{n-1} + r_n \geq V_3 + V_3 = V_4, \\
& r_{n-3} \geq r_{n-2} + r_{n-1} \geq V_4 + V_3 = V_5, \\
& \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
& r_2 \geq r_3 + r_4 \geq V_{n-1} + V_{n-2} = V_n, \\
& b = r_1 \geq r_2 + r_3 \geq V_n + V_{n-1} = V_{n+1}.
\end{aligned}$$

Thus after using n-divisions in Euclidean algorithm, we have $b \geq_{n+1}$. Taking advantage of Theorem 2.4.5, we obtain $V_{n+1} > \alpha^{n-1}$ for $n > 2$ where $\alpha = \frac{1+\sqrt{5}}{2}$. Hence $b > \alpha^{n-1}$. Here, we note that

$$\log b > (n-1)\log\alpha > \frac{n-1}{5}, [\because \frac{1}{5} < \log\alpha]$$

It gives, $n-1 < 5\log b$. Consider b to have k decimal digits. Then $b < 10^k$ and $\log b < k$, which further implies $(n-1) < 5k$. □

Theorem 14.1.7. *Zeckendorf representation: Any positive integer can be expressed as a sum of distinct Fibonacci numbers, no two of which are consecutive.*

Proof. Because two consecutive numbers of the Fibonacci sequence may be combined to give the next one, it is pointless to have consecutive Fibonacci numbers in the representation of an integer. Thus, whenever possible, $V_k + V_{k-1}$ is replaced by V_{k+1} in the following proof.

We proceed by principles of mathematical induction on $n > 2$. Its suffices to show that the integers from the set $\{1, 2, 3, 4, \dots, V_{n-1}\}$ is a sum of numbers from the set $\{V_i | i = 1, 2, 3 \dots, n-2\}$, repetition being not allowed. Consider the first 10 positive integers.

$$\begin{aligned} 1 &= V_1 & 6 &= V_1 + V_3 + V_4 = V_2 + V_3 + V_4 \\ 2 &= V_3 & 7 &= V_3 + V_5 = V_1 + V_2 + V_3 + V_4 \\ 3 &= V_4 & 8 &= V_4 + V_5 \\ 4 &= V_1 + V_4 & 9 &= V_1 + V_4 + V_5 \\ 5 &= V_3 + V_4 & 10 &= V_3 + V_4 + V_5 . \end{aligned}$$

So the theorem prevails for first few positive integers. Suppose the statement is true for $n = k$. Select N in such a way that

$$V_k - 1 < N < V_{k+1}.$$

Since, $N - V_{k-1} < V_{k+1} - V_{k-1} = V_k$ it implies $N - V_{k-1}$ is representable as a sum of distinct numbers from the set $\{V_i | i = 1, 2, 3 \dots, k-2\}$. Consequently, N and the integers from the set $\{1, 2, 3, 4, \dots, V_{k+1} - 1\}$ can be written, without repetition, as a sum of numbers from the set $\{V_i | i = 1, 2, 3 \dots, k-2, k-1\}$. Hence we are done. □

Theorem 14.1.8. *Binet formula: For any integer $n \geq 1$,*

$$V_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

Proof. To begin with, consider the quadratic equation

$$x^2 - x - 1 = 0. \tag{14.1.4}$$

Let γ and δ be the roots of (14.1.4). Then $\gamma = \dfrac{1+\sqrt{5}}{2}$ and $\delta = \dfrac{1-\sqrt{5}}{2}$. Since γ and δ are the roots of (14.1.4), therefore

$$\gamma^2 - \gamma - 1 = 0 \tag{14.1.5}$$

$$\delta^2 - \delta - 1 = 0. \tag{14.1.6}$$

Multiplying (14.1.5) by γ^n and (14.1.6) by δ^n, we obtain

$$\gamma^{n+2} - \gamma^{n+1} - \gamma^n = 0 \tag{14.1.7}$$

$$\delta^{n+2} - \delta^{n+1} - \delta^n = 0. \tag{14.1.8}$$

Now, $\{(14.1.7) - (14.1.8)\}/(\gamma - \delta)$ gives

$$\frac{\gamma^{n+2} - \delta^{n+2}}{\gamma - \delta} = \frac{\gamma^{n+1} - \delta^{n+1}}{\gamma - \delta} + \frac{\gamma^n - \delta^n}{\gamma - \delta}.$$

Set $V_n = \dfrac{\gamma^n - \delta^n}{\gamma - \delta}$. Then the foregoing equation can be simplified as,

$$V_{n+2} = V_{n+1} + V_n, n \geq 1.$$

Since γ and δ are the roots of the (14.1.4) therefore from the relation between roots and coefficients we have

$$\gamma + \delta = 1,\ \gamma\delta = -1,\ \gamma - \delta = \sqrt{5}.$$

Thus, $V_1 = 1$, $V_2 = 1$, $V_3 = 2$, $V_4 = 3$ and so on. Hence $\{V_1, V_2, V_3, \ldots\}$ forms a Fibonacci sequence, where the nth term of the sequence is given by $V_n = \dfrac{\gamma^n - \delta^n}{\gamma - \delta}$. □

An immediate consequence of Binet formula is the following two identities:

Theorem 14.1.9. *For* $n \geq 1$, $V_{n+2}^2 - V_n^2 = V_{2(n+1)}$.

Proof. Since $\gamma\delta = -1 \Rightarrow (\gamma\delta)^{2k} = 1$, for $k \geq 1$. Also, $\gamma + \delta = 1$. Then,

$$\begin{aligned} V_{n+2}^2 - V_n^2 &= \left[\frac{\gamma^{n+2} - \delta^{n+2}}{\gamma - \delta}\right]^2 - \left[\frac{\gamma^n - \delta^n}{\gamma - \delta}\right]^2 \\ &= \frac{\gamma^{2(n+2)} + \delta^{2(n+2)} - \gamma^{2n} - \delta^{2n}}{(\gamma - \delta)^2} \\ &= \frac{(\gamma^2 - \delta^2)(\gamma^{2(n+1)} - \delta^{2(n-1)})}{(\gamma - \delta)^2} \\ &= (\gamma + \delta)V_{2(n+1)} = V_{2(n+1)}. \end{aligned}$$

Hence proved. □

Theorem 14.1.10. *For any integer* $n \geq 1$, $V_{2n+1}V_{2n-1} - 1 = V_{2n}^2$.

Proof. Since $\gamma\delta = -1 \Rightarrow (\gamma\delta)^{2k} = 1$, for $k \geq 1$. Also, $\gamma^2+\delta^2 = (\gamma+\delta)^2 - 2\gamma\delta = 3$. Then,

$$\begin{aligned}
V_{2n+1}V_{2n-1} - 1 &= \left[\frac{\gamma^{2n+1} - \delta^{2n+1}}{\gamma - \delta}\right]\left[\frac{\gamma^{2n-1} - \delta^{2n-1}}{\gamma - \delta}\right] - 1\\
&= \left[\frac{\gamma^{2n+1} - \delta^{2n+1}}{\sqrt{5}}\right]\left[\frac{\gamma^{2n-1} - \delta^{2n-1}}{\sqrt{5}}\right] - 1\\
&= \frac{\gamma^{4n} + \delta^{4n} + (\gamma^2 + \delta^2) - 5}{5}\\
&= \frac{\gamma^{4n} + \delta^{4n} - 2}{5}\\
&= \frac{\gamma^{4n} + \delta^{4n} - 2(\gamma\delta)^{2n}}{5}\\
&= \left[\frac{\gamma^{2n} - \delta^{2n}}{\sqrt{5}}\right]^2 = V_{2n}^2.
\end{aligned}$$

□

Before retiring from the field, the remaining theorems of this section deals with the prime factors of Fibonacci numbers.

Theorem 14.1.11. *For a prime* $p > 5$, *either* $p|V_{p-1}$ *or* $p|V_{p+1}$ *but not both.*

Proof. Using Binet's formula we get, $V_p = \frac{(\alpha^p - \alpha_2^p)}{\sqrt{5}}$. If we expand p-th power of α and α_2 by the binomial theorem then we obtain,

$$\begin{aligned}
V_p &= \frac{1}{2^p\sqrt{5}}[1 + \binom{p}{1}\sqrt{5} + \binom{p}{2}5 + \cdots + \binom{p}{p}5^{\frac{p-1}{2}}\sqrt{5}]\\
&\quad - \frac{1}{2^p\sqrt{5}}[1 - \binom{p}{1}\sqrt{5} + \binom{p}{2}5 - \cdots - \binom{p}{p}5^{\frac{p-1}{2}}\sqrt{5}]\\
&= \frac{1}{2^{p-1}}[\binom{p}{1} + \binom{p}{3}5 + \binom{p}{5}5^2 + \cdots + \binom{p}{p}5^{\frac{p-1}{2}}].
\end{aligned}$$

Now using the facts that $\binom{p}{k} \equiv 0(\bmod p)$ for $1 \leq k \leq p-1$ and $2^{p-1} \equiv 1(\bmod p)$ we get,

$$V_p \equiv 2^{p-1}V_p \equiv \binom{p}{p}5^{\frac{p-1}{2}} \equiv 5^{\frac{p-1}{2}}(\bmod p).$$

Now since $\gcd(5, p) = 1$, then by Fermat's little theorem $5^{p-1} \equiv 1(\bmod p)$. This shows $V_p^2 \equiv 1(\bmod p)$. Now if we apply an well known identity $V_p^2 = V_{p-1}V_{p+1} + (-1)^{p-1}$ modulo p then we have, $V_{p-1}V_{p+1} \equiv 0(\bmod p)$. As $p > 5$ then $\gcd(p-1, p+1) = 2$ and applying Theorem 14.1.3 together we have found that $\gcd(V_{p-1}, V_{p+1}) = V_2 = 1$.

Finally we can conclude that either $p|V_{p-1}$ or $p|V_{p+1}$ but not both. □

Theorem 14.1.12. *Let $p \geq 7$ be a prime satisfying $p \equiv 2(\bmod 5)$ or $p \equiv 4(\bmod 5)$ then $2p-1$ divides V_p provided $2p-1$ is prime.*

Proof. Let p is of the form $5k+2$ for some integer k. Now from Binet's formula we have, $V_p = \frac{(\alpha^p - \beta^p)}{\sqrt{5}}$. $V_p = \frac{(\alpha^p - \alpha_2^p)}{\sqrt{5}}$. Squaring both sides and expanding α^{2p} and α_2^{2p} by

$$5V_p^2 = \frac{1}{2^{2p-1}}\left[1 + \binom{2p}{2}5 + \binom{2p}{4}5^2 + \cdots + \binom{2p}{2p}5^p\right] + 2.$$

Since $2p-1$ is a prime then by Fermat's little theorem we have $2^{(2p-1)-1} \equiv 1(\bmod 2p-1)$ or $2^{2p-1} \equiv 2(\bmod 2p-1)$. Also $\binom{2p}{k} \equiv 0(\bmod 2p-1)$ for $2 \leq k < 2p-1$. Applying these two facts together the above expression reduces to,

$$2(5V_p^2) \equiv (1 + 5^p) + 4(\bmod 2p-1)$$

or

$$2V_p^2 \equiv 1 + 5^{p-1}(\bmod 2p-1).$$

Now, $5^{p-1} = 5^{\frac{2p-2}{2}} \equiv (\frac{5}{2p-1})(\bmod 2p-1)$[by Euler's criterion]. Again from Corollary 9.4.2 it is clear that,

$$\left(\frac{5}{2p-1}\right) = \left(\frac{2p-1}{5}\right) = \left(\frac{10k+3}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Thus we have, $2V_p^2 \equiv 1 + (-1)(\bmod 2p-1)$. This shows that $2p-1$ divides V_p. If $p \equiv 4(\bmod 5)$ then $p = 5k' + 4$ for some integer k'. Then applying the Corollary 9.4.2 again we see that,

$$\left(\frac{5}{2p-1}\right) = \left(\frac{2p-1}{5}\right) = \left(\frac{10k'+7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Then we have, $2V_p^2 \equiv 1 + (-1)(\bmod 2p-1)$. This also shows that $2p-1$ divides V_p. □

14.2 Worked out Exercises

Problem 14.2.1. *Show that the sum of squares of the first n Fibonacci numbers is given by,*

$$V_1^2 + V_2^2 + \cdots + V_n^2 = V_n V_{n+1}.$$

Solution 14.2.1. *Let us consider, $V_t V_{t+1} - V_{t-1} V_t = V_t(V_{t+1} - V_{t-1}) = V_t^2$ for $t \geq 2$.*

Now taking $t = 1, 2, 3, \cdots, n$ *we have,*

$$\begin{aligned} V_1^2 &= V_1 V_2 \\ V_2^2 &= V_2 V_3 - V_1 V_2 \\ V_3^2 &= V_3 V_4 - V_2 V_3 \\ \vdots &= \vdots \\ V_n^2 &= V_n V_{n+1} - V_{n-1} V_n. \end{aligned}$$

Adding those equations we get,

$$V_1^2 + V_2^2 + \cdots + V_n^2 = V_n V_{n+1}.$$

Problem 14.2.2. *Evaluate* $\gcd(V_{15}, V_{20})$.

Solution 14.2.2. *From Theorem 14.1.3 it is clear that* $\gcd(V_m, V_n) = V_d$ *where* $d = \gcd(m, n)$. *Now here* $\gcd(15, 20) = 5$ *then* $\gcd(V_{15}, V_{20}) = V_5 = 5$.

Problem 14.2.3. *If* $\gcd(m, n) = 1$, *prove that* $V_m V_n \big| V_{mn} \ \forall\, m, n \geq 1$.

Solution 14.2.3. *As* $m, n \geq 1$ *then applying Theorem 14.1.2 we can say that* $V_m | V_{mn}$ *and* $V_n | V_{mn}$. *Since* $\gcd(m, n) = 1$, *then we have* $\gcd(V_m, V_n) = V_1 = 1$. *Thus applying Corollary 2.4.1 we can conclude that* $V_m V_n | V_{mn}$ *for all* $m, n \geq 1$.

Problem 14.2.4. *Show that* $V_{2n+1} = V_{n+1}^2 + V_n^2$ *whenever* n *is a positive integer.*

Solution 14.2.4. *We will solve this problem by the principle of mathematical induction. For this let us assume* $n = 1$. *Then we have* $V_3 = 2 = V_2^2 + V_1^2 = 1 + 1$. *If we choose* $n = 2$ *then we get,* $V_5 = 5 = 2^2 + 1^2 = V_3^2 + V_2^2$. *Thus the result is true for* $n = 1, 2$. *Now we have to assume that the identity is true for all* n *less than or equal to* k. *Then we can assume that* $V_{2k-3} = V_{k-1}^2 + V_{k-2}^2$ *and* $V_{2k-1} = V_k^2 + V_{k-1}^2$. *Finally we need to calculate* V_{2k+1}. *Thus,*

$$\begin{aligned} V_{2k+1} &= V_{2k} + V_{2k-1} \\ &= V_{2k-1} + V_{2k-2} + V_{2k-1} \\ &= 2V_{2k-1} + (V_{2k-1} - V_{2k-3}) \\ &= 3V_{2k-1} - V_{2k-3}. \end{aligned}$$

Now substituting all the assumptions in above equation we get,

$$\begin{aligned} V_{2k+1} &= 3(V_k^2 + V_{k-1}^2) - (V_{k-1}^2 + V_{k-2}^2) \\ &= 3V_k^2 + 2V_{k-1}^2 - (V_k - V_{k-1})^2 \\ &= 2V_k^2 + V_{k-1}^2 + 2V_k V_{k-1} \\ &= 2V_k^2 + (V_{k+1} - V_k)^2 + 2V_k(V_{k+1} - V_k) \\ &= V_{k+1}^2 + V_k^2. \end{aligned}$$

Now by applying principle of mathematical induction we can say that the result is true for all positive integer n.

Problem 14.2.5. *Show that the simple continued fraction, terminating with the partial quotient of* 1, *of* $\dfrac{V_{k+1}}{V_k}(k \in \mathbb{Z}^+)$ *is* $[1; 1, 1, 1 \ldots, 1]$*(k-times) where* V_k *denote the k-th Fibonacci number.*

Solution 14.2.5. *In view of recursion formulae for the Fibonacci sequence, the Euclidean algorithm for* $\dfrac{V_{k+1}}{V_k}$ *yields;*

$$\begin{aligned} V_{k+1} &= 1(V_k) + V_{k-1} \\ V_k &= 1(V_{k-1}) + V_{k-2} \\ \vdots &= \vdots \\ V_2 &= 1(V_1). \end{aligned}$$

So $\dfrac{V_{k+1}}{V_k} = [1; 1, 1, 1 \ldots, 1]$*($k$-times). Hence the proof.*

Problem 14.2.6. *Prove that the sum of the first n Fibonacci numbers with odd indices is given by the formula*

$$V_1 + V_3 + V_5 + \cdots + V_{2n-1} = V_{2n}.$$

Solution 14.2.6. *We will prove this formula by principle of mathematical induction. Here we can see that,* $V_1 = V_2 = 1,\ V_1 + V_3 = 3 = V_4$. *So the identity is true for* $n = 1$ *and* $n = 2$. *Let us assume that the identity is true for* $n = k$. *We now show that the identity is true for* $n = k + 1$.*Here,*

$$\begin{aligned} V_1 + V_3 + V_5 + \cdots + V_{2n-1} &= V_{2k} + V_{2k+1} \text{ [by induction hypothesis]} \\ &= V_{2k+2}. \end{aligned}$$

Thus the result is true for $n = k + 1$. *So by principle of mathematical induction we can say that the result is true for all positive odd integer n.*

Problem 14.2.7. *Find the Zeckendorf representation of* 50 *and* 110.

Solution 14.2.7. *Zeckendorf representation we can assert that any positive integer can be expressed as a sum of distinct Fibonacci numbers, no two of which are consecutive. Here,* $50 = 34+13+3 = V_9+V_7+V_4$ *and* $110 = 89+21 = V_{11}+V_8$.

Problem 14.2.8. *From the Binet's formula of Fibonacci numbers, derive the relation*

$$V_{2n+2}V_{2n-1} - V_{2n}V_{2n+1} = 1,\ n \geq 1.$$

Solution 14.2.8. *From Binet's formula we have,* $V_n = \frac{\alpha_1^n - \beta_1^n}{\sqrt{5}}$ *where* $\alpha_1 + \beta_1 = 1$, $\alpha_1\beta_1 = -1$, $\alpha_1 - \beta_1 = \sqrt{5}$. *Now*

$$\begin{aligned}
V_{2n+2}V_{2n-1} - V_{2n}V_{2n+1} &= \frac{\alpha_1^{2n+2} - \beta_1^{2n+2}}{\sqrt{5}} \times \frac{\alpha_1^{2n-1} - \beta_1^{2n-1}}{\sqrt{5}} \\
&\quad - \frac{\alpha_1^{2n} - \beta_1^{2n}}{\sqrt{5}} \times \frac{\alpha_1^{2n+1} - \beta_1^{2n+1}}{\sqrt{5}} \\
&= \frac{\alpha_1^{4n+1} - \alpha_1^{2n+2}\beta_1^{2n-1} - \alpha_1^{2n-1}\beta_1^{2n+2} + \beta_1^{4n+1}}{5} \\
&\quad - \frac{\alpha_1^{4n+1} - \alpha_1^{2n}\beta_1^{2n+1} - \alpha_1^{2n+1}\beta_1^{2n} + \beta_1^{4n+1}}{5} \\
&= \frac{\alpha_1^{2n}\beta_1^{2n+1} + \alpha_1^{2n+1}\beta_1^{2n} - \alpha_1^{2n+2}\beta_1^{2n-1} - \alpha_1^{2n-1}\beta_1^{2n+2}}{5} \\
&= \frac{\alpha_1^{2n}\beta_1^{2n}[(\alpha_1 + \beta_1) - (\frac{\alpha_1^2}{\beta_1} + \frac{\beta_1^2}{\alpha_1})]}{5} \\
&= \frac{\alpha_1\beta_1 - \{(\alpha_1 + \beta_1)^3 - 3\alpha_1\beta_1(\alpha_1 + \beta_1)\}}{5\alpha_1\beta_1} \\
&= \frac{-1 - (1+3)}{-5} = 1.
\end{aligned}$$

14.3 Pseudo-random Numbers

Randomly chosen numbers are very much useful for performing computer simulations of some complicated statistical or mathematical phenomena. But the methods commonly used to generate random numbers are not a random process. Random numbers are called pseudo-random numbers when they are generated by some deterministic process but they qualify the predetermined statistical test for randomness. The first input will determine the sequence of Pseudo random numbers generated by any method of determining them. One such method is called mid-square method. This method was first introduced by Von Neumann in the year 1949.

Mid-square method

Mid-Square method was the first method used to generate Pseudo random numbers. In order to generate a sequence of Pseudo random numbers, we need to select a number with n digits. Then squaring that n-digit number, the next number will be the middle part of that squared number. For better explanation, let us consider a four digit number. Subsequently, we are to square this four digit number. From this squared digit number we need to take out the middle four digit. This will give us the second random number. After that we are to iterate this method to obtain a sequence of random numbers. Here we need to remember certain things. We know that the square of a four digit number has eight digits or fewer than this. Those fewer than eight digits has to be considered as eight digit number by adding zero as initial digit or digits. However the sequence of numbers produced in this method appears to be random, and they are useful for computer simulations. This sequence of random numbers are called pseudo random numbers.

Let us illustrate the above discussion with an example. Take a two digit number 69 as the seed. So 69 is our initial approximation. Squaring 69 we get $69^2 = 4761$. On applying mid-square method we obtain 76 as second term. The third term is 77 as $76^2 = 5776$. Continuing this way we will get thirteenth term 05 as $84^2 = 7056$. Then the fourteenth term will be 02 as $5^2 = 25 = 0025$. This process will be terminated at sixteenth term as $2^2 = 4 = 0004$ and the middle two digits will become 00.

Some discrepancies lies with the Mid-Square method. The most undesirable feature is that this process produces small set of random numbers. For instance, the last example shows that after sixteenth stage the random numbers will occur only zero. So to overcome this drawback we need an algorithm, known as Linear Congruential Method, for finding pseudo-random numbers.

Linear Congruential Method

To begin with, consider some integers $a,\ c,\ m$ with the constraints $m > 0,\ 2 \leq a < m,\ 0 \leq c \leq m$. Select the seed x_0 such that $0 \leq x_0 \leq m$. To obtain the sequence of pseudo random numbers, we need to construct the recursive congruence relation

$$x_{n+1} \equiv ax_n + c(\mod m);\ 0 \leq x_{n+1} < m, \quad \text{for } n = 0, 1, 2, \ldots.$$

Note that m is modulus, a is multiplier and c is the increment. The following example will lucidly illustrate the method.

Example 14.3.1. *Consider* $m = 19,\ a = 5$ *and* $c = 2$. *If we take the seed*

$x_0 = 6$, *then from* $x_{n+1} \equiv ax_n + c(\bmod m)$ *we get*

$$\begin{aligned}
x_1 &\equiv 5 \times 6 + 2 \equiv 32(\bmod 19) && \Rightarrow x_1 \equiv 13(\bmod 19)\\
x_2 &\equiv 5 \times 13 + 2 \equiv 67(\bmod 19) && \Rightarrow x_2 \equiv 10(\bmod 19)\\
x_3 &\equiv 5 \times 10 + 2 \equiv 52(\bmod 19) && \Rightarrow x_3 \equiv 14(\bmod 19)\\
x_4 &\equiv 5 \times 14 + 2 \equiv 72(\bmod 19) && \Rightarrow x_4 \equiv 15(\bmod 19)\\
x_5 &\equiv 5 \times 15 + 2 \equiv 77(\bmod 19) && \Rightarrow x_5 \equiv 1(\bmod 19)\\
x_6 &\equiv 5 \times 1 + 2 \equiv 7(\bmod 19) && \\
x_7 &\equiv 5 \times 7 + 2 \equiv 7(\bmod 19) && \Rightarrow x_7 \equiv 18(\bmod 19)\\
x_8 &\equiv 5 \times 18 + 2 \equiv 92(\bmod 19) && \Rightarrow x_8 \equiv 16(\bmod 19)\\
x_9 &\equiv 5 \times 16 + 2 \equiv 82(\bmod 19) && \Rightarrow x_9 \equiv 6(\bmod 19)\\
x_{10} &\equiv 5 \times 6 + 2 \equiv 32(\bmod 19) && \Rightarrow x_{10} \equiv 13(\bmod 19).
\end{aligned}$$

So we see that $x_1 \equiv x_{10} \equiv 13(\bmod 19)$. *Hence it follows that* $x_k = x_{k-9}$ *for* $k \geq 10$. *Thus the sequence is* $13, 10, 14, 15, 1, 7, 18, 16, 6, 13, \ldots$ *and it contains* 9 *different numbers.*

The following theorem suggest us to find the terms of the sequence of pseudo random numbers generated by the linear congruential method directly from seed, multiplier and increment.

Theorem 14.3.1. *The terms of the sequence generated by linear congruential method are given by,*

$$x_n \equiv a^n x_0 + \frac{c(a^n - 1)}{(a-1)}\big(\bmod m\big),\ 0 \leq x_n < m.$$

Proof. We can prove the result by mathematical induction on n. For $n = 1$ we get, $x_1 \equiv ax_0 + c(\bmod m)$, $0 \leq x_1 < m$. This is true from the formula of linear congruential method. Let us assume that the result be true for $n = k$. Then the congruence relation $x_k \equiv a^k x_0 + \frac{c(a^k-1)}{(a-1)}\big(\bmod m\big)$, holds for $0 \leq x_k < m$. Since $x_{k+1} \equiv ax_k + c(\bmod m)$, $0 \leq x_{k+1} < m$ holds, then we have

$$\begin{aligned}
x_{k+1} &\equiv a\Big[a^k x_0 + \frac{c(a^k - 1)}{(a-1)}\Big] + c(\bmod m)\\
&\equiv a^{k+1}x_0 + c\Big[\frac{a(a^k - 1)}{(a-1)} + 1\Big](\bmod m)\\
&\equiv a^{k+1}x_0 + c\Big[\frac{(a^{k+1} - 1)}{(a-1)}\Big](\bmod m).
\end{aligned}$$

This shows that the result is true for $n = k+1$. So by principle of mathematical induction we can say that the result is true for all integers n. □

In the Example 14.3.1 we have seen that the sequence of pseudo random numbers contain 9 different numbers for the sequence $13, 10, 14, 15, 1, 7, 18, 16, 6, 13, \ldots$. Here the total number of different elements in the sequence is called period length and is defined as follows.

Definition 14.3.1. *The maximum length of the sequence obtained without repetition in a linear congruential pseudo random number generator is called period length.*

We can see that the longest possible length for a linear congruential generator is the modulus m. In the next theorem, we have given light on this fact. This is also a characterisation theorem of a good generator.

Theorem 14.3.2. *The linear congruential pseudo random number generator produces a sequence of period length m if and only if* $\gcd(c, m) = 1$, $a \equiv 1(\bmod p)$ *for all primes p dividing m, and* $a \equiv 1(\bmod 4)$ *provided* $4 \big| m$.

The proof of this theorem beyond the scope of the book. For further reference see Knuth[8].

In particular if $c = 0$ in the recursive relation $x_{n+1} \equiv ax_n + c(\bmod m)$, then we get the relation as $x_{n+1} \equiv ax_n(\bmod m)$, $0 < x_{n+1} < m$. Here m is the modulus and a is the multiplier. This method is called the pure multiplicative congruential method. Here the terms of the sequence of pseudo random numbers are obtained by $x_n \equiv a^n x_0(\bmod m)$ with $0 < x_{n+1} < m$, where x_0 is the seed.

If L is the period length of the sequence of pseudo random numbers obtained recursively by pure multiplicative congruential method, then L is the least universal exponent. The following proposition indicates this fact.

Proposition 14.3.1. *The largest possible period length of the sequence of pseudo random numbers, generated recursively using pure multiplicative generator is $\lambda(m)$, where $\lambda(m)$ is the least universal exponent modulo m.*

Proof. Let L be the period length of the sequence of pseudo random numbers generated recursively using pure multiplicative generator. Then $x_0 \equiv a^L x_0(\bmod m)$, where a is the multiplier and x_0 is the seed. Now $\gcd(x_0, m) = 1$ yields $a^L \equiv 1(\bmod m)$. An appeal to the definition of least universal exponent, the forgoing congruence relation implies that the largest possible period length is $\lambda(m)$. □

We conclude this section with another method of pseudo random generator. In this method, we need to consider a positive integer m as modulus and the initial term x_0 as seed of the generator. Here the sequence of pseudo random numbers has been generated by the congruence relation,

$$x_{n+1} \equiv x_n^2 (\mod m),\ 0 < x_{n+1} < m.$$

14.4 Worked out Exercises

Problem 14.4.1. *Apply the mid square method for generating pseudo random numbers for* 6139*.*

Solution 14.4.1. *Here the initial seed is* 6139*. Squaring* 6139 *gives* $(6139)^2 = 37687321$*. Applying mid square method, we get* $x_2 = 6873$*. Furthermore, squaring and thereby applying this method we find* $x_3 = 2381$*. Similarly we get* $x_4 = 6691,\ x_5 = 7694,\ x_6 = 1976,\ x_7 = 9045$ *and so on.*

Problem 14.4.2. *Find the period length of the sequence of pseudo random numbers generated by linear congruential method with* $x_0 = 2$ *and* $x_{n+1} \equiv 4x_n + 7(\mod 25)$*.*

Solution 14.4.2. *Here the initial seed* $x_0 = 2$*. Then applying linear congruential method we have,*

$$\begin{array}{ll}
x_1 \equiv 4 \times 2 + 7 \equiv 15(\mod 25) & \Rightarrow x_2 \equiv 4 \times 15 + 7 \equiv 17(\mod 25) \\
\Rightarrow x_3 \equiv 4 \times 17 + 7 \equiv 0(\mod 25) & \Rightarrow x_4 \equiv 4 \times 0 + 7 \equiv 7(\mod 25) \\
\Rightarrow x_5 \equiv 4 \times 7 + 7 \equiv 10(\mod 25) & \Rightarrow x_6 \equiv 4 \times 10 + 7 \equiv 22(\mod 25) \\
\Rightarrow x_7 \equiv 4 \times 22 + 7 \equiv 20(\mod 25) & \Rightarrow x_8 \equiv 4 \times 20 + 7 \equiv 12(\mod 25) \\
\Rightarrow x_9 \equiv 4 \times 12 + 7 \equiv 5(\mod 25) & \Rightarrow x_{10} \equiv 4 \times 5 + 7 \equiv 2(\mod 25).
\end{array}$$

Thus the period length is 10*.*

Problem 14.4.3. *Find the multiplier* a *of a linear congruential generator* $x_{n+1} \equiv ax_n + c(\mod m)$ *for which the period length is* $m = 2^{25} - 1$*, where* $\gcd(c, m) = 1$*.*

Solution 14.4.3. *We have* $2^{25} - 1 = 31 \cdot 601 \cdot 1801$*. Taking into account Theorem 14.3.2, we can say that* $a \equiv 1(\mod p)$ *for* $p = 31,\ 601,\ 1801$*. Finally using Chinese Remainder Theorem we get* $a \equiv 1(\mod 2^{25} - 1)$*.*

Problem 14.4.4. *Using linear congruential method if either* $a = 0$ *or* $a = 1$ *is applied for multiplier in the generation of pseudo random numbers, then prove that the resulting sequence fails to an effective option for the same.*

Solution 14.4.4. *If* $a = 0$ *we have* $x_{n+1} \equiv c (\bmod m)$ *which means that the sequence is constant for* $n \geq 1$. *This is not an effective choice for the sequence of pseudo random numbers. If* $a = 1$ *we have* $x_{n+1} \equiv x_n + c (\bmod m)$, *shows that the terms of the sequence differ by a constant modulo* m. *This is also not an effective choice for the sequence of pseudo random numbers.*

Problem 14.4.5. *Find the sequence of numbers generated by the square pseudo random number generator with modulus* 77 *and seed* 8.

Solution 14.4.5. *Here the initial seed is* $x_0 = 8$ *and the modulus is* $m = 77$. *Then we have,*

$$\begin{aligned} x_1 &\equiv 8^2 \equiv 64(\bmod 77) \\ x_2 &\equiv 64^2 \equiv 15(\bmod 77) \\ x_3 &\equiv 15^2 \equiv 71(\bmod 77) \\ x_4 &\equiv 71^2 \equiv 36(\bmod 77) \\ x_5 &\equiv 36^2 \equiv 64 \equiv x_1(\bmod 77). \end{aligned}$$

Thus the sequence of pseudo random number is $8, 64, 15, 71, 36, 64, \cdots$.

14.5 Cryptology

From ancient times coding and decoding of messages are two very familiar words. With the passage of time, the significance of coding and decoding increases. In defence, the secret communication plays a key role. Now a days the privacy of data is needed for bank and any other financial transactions. In twenty first century, communications through social media creates a huge impact in our daily life. Essence of secured and encrypted medium is a vital issue for these types of communications. Hence there is a great deal of interest in the techniques of making messages unintelligible to everyone except the intended receiver. Many mathematicians and computer scientists have given their important contribution towards the growth of the discipline devoted to secrecy systems called cryptography. Cryptography is the part of cryptology that deals with design and application of secrecy system and cryptoanalysis is aimed at breaking these systems. Actually the word cryptography is the combination of two Greek words 'Krypto'means 'hidden'and 'Graphein'means 'to write'.

In simple words, a message that is to be altered into a secret form is called plaintext while after transformation to a secret form, these messages is said to be ciphertext. The process of converting a plaintext to a ciphertext is called encrypting and the reverse process of converting from ciphertext to plaintext is said to be decrypting or deciphering. A cipher is a method for altering a plaintext message to ciphertext by changing the letters of plaintext using a transformation. This section is devoted with few types of methods of encryption and decryption.

One of the most ancient Cryptographic method, first introduced by great Roman emperor Julius Caesar, is called Character or Monographic cipher. Here we will discuss the newest form of Caesar cipher which was invented in late 1970's.

The method starts with translating English alphabetical letters to integers from 0 to 25, as shown in the table below.

Letters	A	B	C	D	E	F	G	H	I	J	K	L	M
Integers	0	1	2	3	4	5	6	7	8	9	10	11	12
Letters	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Integers	13	14	15	16	17	18	19	20	21	22	23	24	25

The Caesar cipher is categorised as a substitution cipher in which each the alphabet in the plaintext is shifted by a fixed number down the alphabet. To explain this by modular arithmetic, let us consider P to be the numeric equivalent of plaintext letter and C be the numerical equivalent of ciphertext letter. Then we have, $C \equiv P+3(\bmod 26)$ where $0 \leq C \leq 25$ and shifting done by three down the alphabet. According to this cipher, if we want to send a message:

HOW ARE YOU

then we can write this as,

$$7\ 14\ 22\ \ 0\ 17\ 4\ \ 24\ 14\ 20.$$

Taking help of the congruence relation we have,

$$10\ 17\ 25\ \ 3\ 20\ 7\ \ 1\ 17\ 23.$$

Now translating back to letters, we get

KRZ DUH BRX.

This is the message we will send. Now the receiver will decipher it by the congruence relation, $P \equiv C-3 \equiv C+23(\bmod 26)$.

The Caesar cipher is one of the family of similar ciphers described by a shift transformation,

$$C \equiv P+k(\bmod 26),\ 0 \leq C \leq 25.$$

Here k is the number of shifting in alphabetical order.

More generally we will consider the transformation of the type,

$$C \equiv aP + b(\text{mod } 26),\ 0 \leq C \leq 25.$$

Here a, b are integers with $\gcd(a, 26) = 1$. These are called affine transformations. Shift transformations are affine transformations with $a = 1$. Here to conduct the cipher, we need $\gcd(a, 26) = 1$ so that P and C runs through complete system of residues modulo 26. There are $\phi(26) = 12$ possibilities of a and 26 possibilities of b, giving total $12 \times 26 = 312$ types of transformations. Here the relationship of ciphertext to plaintext is given by,

$$P \equiv \overline{a}(C - b)(\text{mod } 26),\ 0 \leq P \leq 25.$$

Here $\overline{a}$ is the inverse of a modulo 26.

The monographic cipher is very simple and insecured. To avoid the vulnerability of monographic cipher, we are going to present block or polygraphic cipher, introduced by Lester S. Hill in 1929. This cipher is also called Hill cipher. Hill cipher uses matrix algebra to encrypt blocks of any desire length, where each block contains plaintext letters of specified length. After the encryption, each block of plaintext letters encrypted to ciphertext letters of same length. Here our discussion starts with digraphic cipher, where each block contains two letters of plaintext and it is to be encrypted to a block of two letters of ciphertext.

First, we are to split the message into two blocks of two letters. If the number of letter is odd, then we are to add a dummy letter 'X' so that the final block contains two letters. Consider a message,

BEWARE OF THE MESSENGER.

We now split it into blocks of two letters as,

BE WA RE OF TH EM ES SE NG ER.

Secondly, we need to translate these blocks into its numerical equivalents. So here we translate them to obtain

1 4 22 0 17 4 14 5 19 7 4 12 4 18 18 4 13 6 4 17.

We are to convert each block of plaintext numbers P_1P_2 into ciphertext numbers C_1C_2 by system of linear congruence modulo 26. The formula is given by,

$$C_1 \equiv aP_1 + bP_2(\text{ mod } 26)$$
$$C_2 \equiv cP_1 + dP_2(\text{ mod } 26)$$

where a, b, c and d are integers.

Here in this example we are going to apply the system,

$$C_1 \equiv 3P_1 + 10P_2 (\mod 26)$$
$$C_2 \equiv 9P_1 + 7P_2 (\mod 26).$$

So by this formula for $P_1 = 1$ and $P_2 = 4$ the ciphertext numbers,

$$C_1 \equiv 3 \cdot 1 + 10 \cdot 4 \equiv 43 \equiv 17 (\mod 26)$$
$$C_2 \equiv 9 \cdot 1 + 7 \cdot 4 \equiv 37 \equiv 11 (\mod 26).$$

Thus the ciphertext numbers obtained for entire message is,

17 11 14 16 13 25 14 5 23 12 2 16 10 6 16 8 21 3 10 25.

Finally we need to translate these blocks into letters,

RL OQ NZ OF XM CQ KG QI VD KZ.

The decrypting process in this cipher system has to be done with the help of Theorem(4.6.1). Here in our example the relationship becomes,

$$P_1 \equiv 21C_1 + 22C_2 (\mod 26)$$
$$P_2 \equiv 25C_1 + 9C_2 (\mod 26).$$

Actually the matrix representation of digraphic cipher is

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \equiv \begin{pmatrix} 3 & 10 \\ 9 & 7 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} (\mod 26)$$

Taking help of proposition(4.6.2) we find the inverse of $\begin{pmatrix} 3 & 10 \\ 9 & 7 \end{pmatrix}$ under modulo 26 is $\begin{pmatrix} 21 & 22 \\ 25 & 9 \end{pmatrix}$ and the relationship becomes,

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} 21 & 22 \\ 25 & 9 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} (\mod 26).$$

In general, the polygraphic cipher where the block length is $n (> 2)$ we need to apply congruences of matrices. Here the matrix relationship becomes,

$$C \equiv AP (\mod 26)$$

where A is an $n \times n$ matrix with $\gcd(\det A, 26) = 1$,

$$\begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{pmatrix} \text{ and } \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{pmatrix}$$

For deciphering we need matrix $\overline{A}$ which is inverse of A modulo 26. This $\overline{A}$ can be obtained by Proposition(4.6.3). Hence to determine the plaintext from ciphertext, we use the relationship,

$$P \equiv \overline{A}C(\mod 26).$$

This polygraphic cipher can only be used for small values of n. For large values of n this method becomes extremely infeasible. In such situation we can carry out our study of Cryptology to another cipher, called exponentiation cipher. This cipher is based on modular exponentiation. This was first introduced by Pohig and Hellman in the year 1978. This is less vulnerable to frequency analysis than block cipher.

To start this procedure, let us consider a prime p and an exponent e first such that $\gcd(e, p-1) = 1$.

Next we have to translate the letters of the message into numerical equivalents. For that we use the relationship given below.

Letters	A	B	C	D	E	F	G	H	I	J	K	L	M
Integers	00	01	02	03	04	05	06	07	08	09	10	11	12
Letters	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Integers	13	14	15	16	17	18	19	20	21	22	23	24	25

After the numeric conversion we need to group the letters in the message in blocks of k letters, where k is chosen so that $\underbrace{2525\cdots25}_{k-\text{times}} < p < \underbrace{2525\cdots25}_{k+1-\text{times}}$. For example if we choose $p = 1423$ then we should use the blocks of $k = 2$ letters, because $2525 < 1423 < 252525$.

Finally we form ciphertext block C from plaintext block P by the relation,

$$C \equiv P^e(\mod p),\ 0 \le C < p.$$

We now illustrate this by an example. For that let us choose $p = 101$ and $e = 3$. We want to encipher the message

G	O	O	D	M	O	R	N	I	N	G
06	14	14	03	12	14	17	13	08	13	06

Since $25 < p < 2525$ then we have to use block of $k = 1$ letters. Now we form ciphertext block from plaintext block by the relation,

$$C \equiv P^3(\mod 101),\ 0 \leq C < 101.$$

This gives us the series,

$$14\ 17\ 17\ 27\ 11\ 17\ 65\ 76\ 07\ 76\ 14.$$

Now to decipher the message that has been encoded using exponential cipher, we need to know the deciphering key an integer d such that $de \equiv 1(\mod p-1)$, so that d is the inverse of e modulo $p-1$. The existence of d has been ensured by the fact that $\gcd(e, p-1) = 1$. Note that de can be written as $de = 1 + n(p-1)$ for some integer n. Now we have,

$$\begin{aligned} C &\equiv P^e(\mod p) \\ \Rightarrow C^d &\equiv P^{ed}(\mod p) \\ &\equiv P \cdot P^{n(p-1)}(\mod p) \\ &\equiv P \cdot (P^{p-1})^n(\mod p). \end{aligned}$$

Using Fermat's little theorem we get,

$$P^{p-1} \equiv 1(\mod p) \text{ as } p \nmid P.$$

Thus we obtain,

$$P \equiv C^d(\mod p).$$

This is the relation for converting encrypted text to plaintext.

The exponentiation cipher has major drawbacks when employed in a network with many users. Here each pair of communicants must employ an enciphering key which is kept secret from the other communicants of that network. The reason is that, if the enciphering key is known then the deciphering key can be obtained by simple computations of number theory. There is another disadvantage of changing encryption key frequently. To avoid those difficulties, we need to assign a key to each pair of individuals which must be kept secret from other individuals of the network. Public Key cipher system has to be introduced to overcome those difficulties.

The aim of public key cipher is to establish secret communications in a network of n individuals. Here each individual produce a key k which is not known to other individuals. We need to pass the private information through the enciphering transformation $E(k)$ for a key k to obtain ciphertext. Now for $k_1, k_2, \cdots k_n$ keys, if the individual i wishes to send a message to individual j

then for plaintext P the ciphertext C is computed by transformation E_{k_j} where $C = E_{k_j}(P)$. To decipher the message, j applies the deciphering transformation D_{k_j} on C to obtain P satisfying $D_{k_j}(C) = D_{k_j}(E_{k_j}(P)) = P$. Today the public key cipher, known as RSA, is the most widely used cipher. In the year 1978, RSA was proposed by Ronald Rivest, Adi Shamir and Leonard Adleman. This public key cipher is based on modular exponentiation.

To construct RSA algorithm, we need to use the keys in pairs (e, n) where e is exponent and n is modulus. Here n must be the product of large primes p and q *i.e.* $n = pq$, so that $\gcd(e, \phi(n)) = 1$. Here consider the integer e satisfying $1 < e < \phi(n)$.

Now to encipher the message, we first translate the letters into numerical using the table described in exponentiation cipher. Finally to encipher a plaintext block P, apply the relation

$$E(P) = C \equiv P^e(\mod n),\ 0 < C < n$$

where C is ciphertext block.

To decipher the ciphertext block C, we need to obtain the inverse exponent d of e modulo $\phi(n)$. The existence of d is ensured by the fact $\gcd(e, \phi(n)) = 1$. Here d and e follow the congruence relation $de \equiv 1(\mathrm{mod}\ \phi(n))$ *i.e.* $de = k'\phi(n) + 1$ for some integer k'. Finally we have,

$$\begin{aligned} D(C) &\equiv C^d \equiv P^{ed}(\mod n) \\ &\equiv P^{k\phi(n)+1}(\mod n) \\ &\equiv (P^{\phi(n)})^k \cdot P \equiv P(\mod n). \end{aligned} \tag{14.5.1}$$

As the probability that P and n not relatively prime is very small, so $\gcd(P, n) = 1$. In view of Euler's theorem, we obtain $P^{\phi(n)} \equiv 1(\mathrm{mod}\ n)$ in congruence (14.5.1). The pair (d, e) is said to be the deciphering key.

Let us exemplify this algorithm with an example. Here we want to encipher the message: BEST WISHES, where $e = 3$ and $n = 2669 = 17 \times 157 = pq$. Now the numeric equivalence of letters of the message is,

$$01\ 04\ 18\ 19\ 22\ 08\ 18\ 07\ 04\ 18.$$

After applying the congruence $C \equiv P^3(\mathrm{mod}\ 2669)$ for $P = 0104$ we have,

$$C \equiv (104)^3 \equiv 1215(\mod 2669).$$

So here the ciphertext is 1215.

Similarly, by means of the last congruence the message becomes,

$$12\ 15\ 12\ 24\ 14\ 71\ 00\ 23\ 01\ 16.$$

14.6 Worked out Exercises

Problem 14.6.1. *Encipher the message: SURRENDER, using the affine transformation* $C \equiv 11P + 18(\mod 26)$.

Solution 14.6.1. *First translate the message into its numerical equivalents,*

S	U	R	R	E	N	D	E	R
18	20	17	17	4	13	3	4	17

Then encipher each numerical equivalence using the relation $C \equiv 11P + 18(\mod 26)$.

For $P = 18,\ C \equiv 11 \times 18 + 18 \equiv 8(\mod 26)$ *and continuing we get,*

8 4 23 23 10 5 25 10 23.

Now translating to letters we have,

I E X X K F Z K X.

Problem 14.6.2. *Decipher the message: RTOLKTOIK, which was encripted by the transformation,* $C \equiv 3P + 24(\mod 26)$.

Solution 14.6.2. *To begin with, convert the transformation by inverse of* 3 *modulo* 26*. Note that* $3 \cdot 9 \equiv 1(\mod 26)$*. Thus* 9 *is inverse of* 3 *modulo* 26*. Now we have,*

$$9(C - 24) \equiv 3 \cdot 9P(\mod 26)$$
$$\therefore P \equiv 9C + 18(\mod 26).$$

Translating the alphabets in numeric we get,

R	T	O	L	K	T	O	I	K
17	19	14	11	10	19	14	8	10

If $C = 17$ *then* $P \equiv 9 \times 17 + 18 \equiv 15(\mod 26)$*. This gives us,*

15 7 14 13 4 7 14 12 4.

and converting back to letters we get, PHONE HOME.

Problem 14.6.3. *Decipher the ciphertext message: UW DM NK QB EK, which was encripted using digraphic cipher which sends the plaintext* P_1P_2 *into ciphertext block* C_1C_2 *with,*

$$C_1 \equiv 23P_1 + 3P_2(\mod 26)$$
$$C_2 \equiv 10P_1 + 25P_2(\mod 26).$$

Solution 14.6.3. *First we translate the message into numeric equivalents,*

$$\begin{array}{cccccccccc} U & W & D & M & N & K & Q & B & E & K \\ 20 & 22 & 3 & 12 & 13 & 10 & 16 & 1 & 4 & 10. \end{array}$$

Now the matrix $\begin{pmatrix} 23 & 3 \\ 10 & 25 \end{pmatrix}$ *has the inverse* $\begin{pmatrix} 1 & 3 \\ 10 & 3 \end{pmatrix}$ *under modulo* 26. *Now for* UW *the plaintext block is,*

$$\begin{pmatrix} 1 & 3 \\ 10 & 3 \end{pmatrix} \begin{pmatrix} 20 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 6 \end{pmatrix} (\bmod 26).$$

Thus UW *has been transferred to* IG. *Similarly transferring other ciphertexts we get,*

IG NO RE TH IS.

Problem 14.6.4. *What is the plaintext message that corresponds to the ciphertext*

12 13 09 02 05 39 12 08 12 34 11 03 13 74 .

produced using modular exponentiation with modulus $p = 2591$ *and enciphering key* $e = 13$*?*

Solution 14.6.4. *Here* $p-1 = 2590$ *and* $13 \cdot 797 \equiv 1 (\bmod 2590)$. *Then* $d = 797$. *Applying the plaintext formula*

$$P \equiv C^{797} (\bmod 2591)$$

we find,

03 14 13 14 19 17 04 00 03 19 07 08 18 23 .

Converting this to letters we get,

DO NO TR EA DT HI SX

where X *is dummy alphabet.*

Problem 14.6.5. *If the ciphertext message:* 05041874034705152088235607360468 *is produced by* RSA *cipher with* $e = 5$ *and* $n = 2881$, *find the plaintext message.*

Solution 14.6.5. *Since* $n = 2881 = 43 \cdot 67$ *and* $\phi(n) = 42 \cdot 66 = 2772$, *the inverse of* 5 *is* 1109 *modulo* $2772 (\because 5 \cdot 1109 \equiv 1 (\bmod 2772))$. *Now we need to take each* 4*-digit block as ciphertext to convert into plaintext using the formula* $P \equiv C^{1109} (\bmod 2881)$. *Calculating congruences for each* 4*-digit block ciphertext we get plaintext block as,* *04 00 19 02 07 14 02 14 11 00 19 04 02 00 10 04 .*

Converting the letters we get,

EA TC HO CO LA TE CA KE.

14.7 Exercises:

1. Prove that $U_{n+3} - U_n = 2U_{n+1}$ whenever n is a positive integer.
2. Evaluate $\gcd(U_{24}, U_{36})$.
3. If 3 divides $n + m$, prove that $U_{n-m-1}U_n + U_{n-m}U_{n+1}$ is an even integer.
4. Show that the sum of the first n Fibonacci numbers with even indices is given by the formula

$$U_2 + U_4 + U_6 + \cdots + U_{2n} = U_{2n+1} - 1.$$

5. Find the Zeckendorf representation of 85 and 200.
6. Find the sequence of pseudo random numbers generated using the middle-square method, taking 369 as the seed.
7. Find the period length of the pure multiplicative pseudo random number generator $x_n \equiv ax_{n-1} (\bmod\ 2^{31} - 1)$ for the multiplier $a = 17$.
8. Find the sequence of numbers generated by the square pseudo random number generator with modulus 1001 and seed 5.
9. Find a good choice for the multiplier a in the pure multiplicative pseudo random number generator $x_{n+1} \equiv ax_n (\bmod\ 101)$.
10. Considering $m = 100,\ a = 17$ and $c = 43$ where the initial seed is $x_0 = 27$, find the sequence of pseudo random numbers using linear congruential method.
11. If the Caesar cipher produced KDSSB ELUWKGDB, what is the plaintext message?
12. Using the linear cipher $C \equiv 5P + 11 (\bmod\ 26)$, encrypt the message NUMBER THEORY IS EASY.
13. Decrypt the message YLF QX PCRIT, which was encrypted using the affine transformation $C \equiv 21P + 5 (\bmod\ 26)$.

14. Using the digraphic cipher that sends the plaintext block P_1P_2 to the ciphertext block C_1C_2, with

$$\begin{aligned} C_1 &\equiv 8P_1 + 9P_2 (\bmod 26) \\ C_2 &\equiv 3P_1 + 11P_2 (\bmod 26), \end{aligned}$$

encrypt the message DO NOT SHOOT THE MESSENGER.

15. What is the ciphertext that is produced when RSA encryption with key $e = 7$ and $n = 2627$ is used to encrypt the message LIFE IS A DREAM?

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Bibliography

[1] Burton,D., Elementary Number Theory, 6th Edition, McGraw-Hill Science/Engineering/Math; 6th edition.

[2] Silverman, J.H., A Friendly Introduction to Number Theory, Pearson; 4th edition(January 28, 2012).

[3] Apostle, Tom, M., Introduction to Analytic Number Theory, Springer.

[4] Rosen, R.K, Elementary Number Theory and its Applications(6th Edition), Pearson Addision Wesely.

[5] Niven, I., Zuckerman, H., An Introduction to the Theory of Numbers(4th Edition), John Wiley & Sons.

[6] Baker, A., A concise Introduction to the Theory of Numbers, Cambridge University Press.

[7] Koblitz, N., A course in number theory and cryptography, 2nd Edition, Springer-Verlag.

[8] Knuth, D.E., Art of Computer Programming: Semi Numerical Algorithms(Vol.2)(2nd Edition), Addision-Wesley; Reading Massachusetts; 1980,

[9] Hill, L.S., Concerning certain linear transformation apparatus of cryptography(Vol.38), American Mathematical Monthly(1931),

[10] CW Coppel, W.A., Number Theory An Introduction to Mathematics: Part A, Springer.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Index

abundant, 247
amicable numbers, 255
amicable pair, 255
arithmetic function, 117
arithmetic progression, 55, 56

Bertrand Conjecture, 64
Binet formula, 328
boundedness, 12

Caesar cipher, 340
Carmichael function, 191
Carmichael numbers, 99
Chinese Remainder Theorem, 84
Chinese remainder theorem, 80
ciphertext, 339
Collatz conjecture, 23
complete residue system, 73
composite, 46, 48, 98, 120
composite numbers, 99
congruence, 68
congruence class, 72
congruence relation, 70
congruent, 68
congruent modulo, 72
consecutive, 136
continued fraction, 266
convergence, 12
coprime, 24, 25
countably infinite, 48
cryptoanalysis, 339
cryptography, 95, 339
Cryptology, 343

deciphering key, 345
decryption, 340
deficient, 247
difference of two squares, 311
Diophantine equation, 37, 275, 300
Diophantine equations, 39
Dirichilet's Theorem, 283
divisible, 16
division algorithm, 17, 133

encryption, 340
equivalence class, 72
equivalence relation, 71
Euclid's Algorithm, 30, 40
Euclid's Lemma, 28
Euclidean Algorithm, 266
Euler polynomial, 56
Euler's Criterion, 205
Euler's generalization, 153
Euler's phi function, 146, 156, 158
exponent, 138
exponential congruence, 198
exponentiation cipher, 343

factorial, 134
factorisation, 114
Fermat number, 257, 260

Fermat prime, 257
Fermat's Last Theorem, 302
Fermat's Little Theorem, 96
Fibonacci number, 325
Fibonacci sequence, 324
finite continued fraction, 266
finite simple continued fraction, 267

Gauss Lemma, 209
geometric series, 124
Golbach's Conjecture, 53
greatest common divisor, 23, 24, 27
greatest integer function, 132
greatest lower bound, 9

Hill cipher, 341

index, 192, 193
infinite continued fractions, 276
integer, 98
irrational, 6, 50, 63

Jacobi symbol, 225

Korselt's Criterion, 99
Kronecker symbol, 234

Lam$\acute{e}'s$ theorem, 327
least common multiple, 31
least universal exponent, 337
least upper bound, 8
Legebdre symbol, 219
Legendre symbol, 206, 249
linear combination, 25, 26
linear congruence, 77, 78, 80, 85, 87, 106, 192
linear congruential generator, 337
linear congruential method, 336
linear Diophantine equation, 77, 78
Liouville function, 140
Lucas-Lehmer Test, 251
lucky numbers, 56

Mö̈bius inversion, 113
mathematical induction, 2
Mersenne number, 99, 247, 248
Mersenne Prime, 248
Mid-Square method, 334
Miller's test, 100
minimal remaider, 21
minimal remainder, 19
Mobiöus Inversion, 160
monographic cipher, 341
monotone decreasing sequence, 13
monotone increasing sequence, 13
multiplicative function, 117, 147
multiplicative property, 116

Pascal's triangle, 5
Pepin's Test, 259
perfect number, 239, 241
period length, 337
periodic fraction, 286
Pigeonhole principle, 5
plaintext, 339
polygraphic cipher, 341
polynomial congruence, 175
polynomial congruences, 290
prime, 46, 114, 134
primitive Pythagorean triple, 296, 297, 302
primitive root, 167, 170, 171, 173, 174
product, 123
pseudo-random numbers, 334
pseudoprime, 98
public-key, 95
pure multiplicative generator, 337
Pythagorean triple, 296

quadratic congruence, 107, 203, 222
quadratic irrational, 286

quadratic non residue, 210
quadratic nonresidue, 204
quadratic reciprocity, 220
Quadratic Reciprocity Law, 217
quadratic reciprocity law, 203
quadratic residue, 204, 205, 208

rational, 50
rational numbers, 6
recursion formulae, 333
reflexive, 71
relatively prime, 117
remainder, 75
residue, 67
RSA algorithm, 345

Sieve of Eratosthenes, 50
simple continued fraction, 333
simple fundamental recurrence relations, 276
simple infinite continued fraction, 277
square free, 99
successive convergents, 274
sum of four squares, 318
sum of three squares, 315
sum of two squares, 308
super perfect number, 247
symmetric, 71

Thue, 308
transitive, 71
triangular number, 243
twin primes, 121

well-ordering, 2
Wilson's theorem, 106

Zeckendorf representation, 328